



159159

A SYSTEM AND METHOD FOR SECURE DELIVERY OF MACHINE READABLE FLASH OVER NETWORKS AND MOBILE PLATFORMS

FIELD OF INVENTION

5

The present invention relates to a system and method for secure delivery of machine readable flash over networks and mobile platforms preventing manipulation and injection to mark machine readable flash for blocking.

BACKGROUND ART

Machine readable flash use permits instruction to translate to small file sizes which may take less bandwidth for transmission. Machine readable flash is blocked on some mobile platforms.

15

A machine readable flash may include content and sequences of machine readable instruction to manipulate the content and handle user interactivity. In a typical environment, machine readable flash may be delivered by a server to a client, which may invoke to execute the machine readable flash. The machine readable instructions, which may be referred to as "action code," may be based on a set of instructions defined on a virtual machine. A sequence of instructions may result from compiling the machine readable flash to generate the action code sequence by other mechanisms. The virtual machine may provide facilities for invoking network communications via action code sequences.

25

Organizations may utilize machine readable flash for a variety of purposes. For example, more and more organizations are adopting machine readable flash in developing corporate media assets and applications. However, in today's world of mobile, blocking machine readable flash content on major mobile platforms has created a major set-back to the industry and the organizations that depend on it. Organizations are forced to downgrade to other lower-end solutions to overcome this problem, resulting in huge investment losses and resource allocations. An existing solution to this problem for machine readable flash content may be machine readable flash emulation, where machine readable flash content is re-routed to a server and converted to other forms.

30



G00001

The invention provides for secure delivery of machine readable flash over networks and mobile platforms by preventing manipulation and injection to mark machine readable flash for blocking purposes.

- 5 The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area where some embodiments described herein may be practice.

SUMMARY OF INVENTION

The present invention relates to a system and method for secure delivery of machine readable flash over networks and mobile platforms preventing manipulation and injection to mark machine readable flash for blocking.

One aspect of the invention provides a system (100) for secure delivery of flash content over networks and mobile platforms. The system (100) comprising at least one client (106) and server (102); and at least one network device (104) comprising at least one bus, processor (202), main memory (204), storage device (208), input device (210), output device (212) and communication interface (214). The said main memory (204) further comprising at least one secure memory location and at least one non-transitory device-readable memory; said secure memory location and said non-transitory device-readable memory having means for receiving machine readable flash via a network; disassembling said machine readable flash into machine readable instructions; locating a portion of the machine readable instructions making a network request associated with the machine readable flash; said secure memory location and said non-transitory device-readable memory whilst locating a portion of the machine readable instructions further examining stack and trace constants of the machine readable instructions to locate a function; determining if said function is associated with making network request associated with machine readable flash; examining machine readable instructions to determine number of arguments for said function whilst said function is making a network request for machine readable flash; rewriting portion of machine readable instructions making the network request to redirect network communication associated with machine readable flash to secure memory location; said secure memory location and said non-transitory device-readable memory whilst rewriting portion of the machine readable instructions further replacing function invocation in the machine readable instructions with a rewriting function to redirect before invoking the function, the network communication associated with the machine readable flash to the secure memory location to prevent any modification in the machine readable flash, re-writing itself back to the original flash file at the execution level to assert originality, and providing secure communication of machine readable flash via network to a client device.

Another aspect of the invention provides a system wherein the at least one non-transitory device-readable memory stores executable instructions for securing delivery of machine readable flash over a network by said non-transitory device-readable memory comprising instructions. The said instructions executed by a processor, cause
5 the processor to determine whether an object of machine readable instruction is of a certain class; executed by said processor, cause the processor to rewrite arguments of said machine readable instruction; executed by said processor, cause the processor to determine whether an application class, of the machine readable instruction implements one or more actions that are unrelated to the network;
10 executed by said processor, cause the processor to inject a machine readable instruction sequence that replaces a statement in the machine readable instructions when said machine readable instruction implements one or more actions that are unrelated to the network; executed by the processor, cause the processor to examine stack and trace constants of the machine readable instruction to locate an action
15 related to making the network request associated with the machine readable flash; executed by the processor, cause the processor to determine a number of arguments for the action; and executed by the processor, cause the processor to replace invocation of the action, in the machine readable instruction, with a rewriting function that redirects before invoking the action, the network communication associated with
20 the flash content to a secure memory location.

A further aspect of the invention provides a system wherein said instructions of said non-transitory device-readable memory further comprising instructions to inject a client-side process into the machine readable instruction.

25 Yet another aspect of the invention provides that said instructions of said non-transitory device-readable memory to inject a client-side process into the machine readable instruction further comprising instructions to determine whether an object of the machine readable instruction is of a certain class; instructions to rewrite
30 arguments of the machine readable instruction, to redirect network communication of the object to the secure memory location, when the object is of the certain class; instructions to determine whether an application class, of the machine readable instruction implements an action unrelated to the network; and instructions to inject a machine readable instruction sequence that replaces a statement in the machine

readable instruction when the application class implements the action unrelated to the network.

Another aspect of the invention provides a system wherein said machine readable instruction includes action codes comprising instructions defined on a virtual machine and said non-transitory device-readable memory further comprising non-transitory readable memory device. The said non-transitory readable memory device may be either a physical device or a virtual device.

10 A further aspect of the invention provides a method for secure delivery of flash content over networks and mobile platforms. The method (300) comprising steps of receiving machine readable flash by a network device (302); disassembling said machine readable flash into machine readable instructions (304); locating a portion of the machine readable instructions making a network request associated with machine
15 readable flash (306) which includes examining stack and trace constants of machine readable instruction to locate a function (308); determining if said function is associated with making the network request associated with said machine readable flash (310); examining machine readable instruction to determine number of arguments for said function when said function is associated with making network
20 request associated with machine readable flash (312); rewriting the portion of the machine readable instruction making the network request to redirect a network communication associated with machine readable flash to the secure memory location (314); injecting a client side process into the machine readable flash where the client side process rewrites the machine readable flash to redirect a network
25 request for a flash object to the secure memory location when the flash object is of a certain class (320); performing flow analysis on the machine readable instruction and inspecting a stack of the machine readable instruction to locate an instruction parameter related to making the network request associated with the machine readable flash (322); rewriting said machine readable instruction parameter to redirect
30 the network communication associated with the machine readable flash to the secure location (324); and replacing the machine readable instruction parameter with the rewritten instruction parameter (326). The step of rewriting the portion of the machine readable instruction making the network request to redirect a network communication associated with executable content to the secure memory location further comprises

steps of replacing a function invocation in the machine readable instruction with a rewriting function to redirect before invoking the function, the network communication associated with the machine readable flash to the secure memory location to prevent any further modification in the machine readable flash, re-writing itself back to the original flash file at the execution level to assert originality (316); and providing secure communication of the flash content, via the network, to a client device (318).

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific
5 embodiments thereof, which are illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

10 FIG. 1 illustrates the architecture of the present invention.

FIG. 2 illustrates the block diagram of the components of the present invention.

FIG. 3 is a flowchart illustrating a method for secure delivery of flash content over
15 networks and mobile platforms.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for secure delivery of machine readable flash over networks and mobile platforms preventing manipulation and injection to mark machine readable flash for blocking.

Hereinafter, this specification will describe the present invention according to the preferred embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned without departing from the scope of the appended claims.

As described more fully below, implementations consistent with principles of the invention relate to intermediation of machine readable flash content for secure delivery over a network. By securing the machine readable flash content as it is being delivered to a client, certain machine readable flash actions that are transmitted via a network by a network server may be modified and protected so that, when loaded into the client, the machine readable flash content may communicate with an intermediate memory allocated segment rather than the device. This may ensure that communication between the client running the machine readable flash content and the network may be captive and secure. Communications between the client running the flash content and the network may be controlled by the intermediate memory allocated segment, and may be performed in a "clientless" manner, i.e., without client-side traffic.

Instead of modifying the machine readable flash content to be blocked by a certain systems, implementations consistent with principles of the invention may directly modify machine readable instructions of the machine readable flash content action code, as it is being delivered to the client, so that machine readable instructions related to network communications may be protected and rewritten to prevent any further modification to the machine readable flash content. Machine readable flash content may be in one implementation consistent with principles of the invention and may adjust the overall instruction sequences to protect and validate the action code of the machine readable flash content making it executable to all devices regardless of any attempt to block it.

Referring to FIG. 1, a system (100) for secure delivery of flash content over networks and mobile platforms of the present invention is illustrated. A single client (106) and a server (102) have been illustrated in FIG. 1 for simplicity. In some instances, client (106) may perform a function of server (102) and server (102) may perform a function of client (106). As illustrated in FIG. 1, a client (106) may connect to a private or public network, which contains a server (102) via public network. Private network may include a local area network (LAN), a private network, such as a company intranet, or another type of network. Private network may also include organizational components, devices, servers, etc. Public network may include a local area network (LAN), a wide area network (WAN), a telephone network, such as the Public Switched Telephone Network (PSTN), other networks, or a combination of networks. Client and/or server may each include a device. In one implementation, client and/or server may take the form of a provider of network content. Server may include a server, or a set of servers.

Referring to FIG. 2, the block diagram of the components of the present invention is illustrated. The system for secure delivery of flash content over networks and mobile platforms comprising a client (106) and a server (102) and a network device (104) comprising a bus, processor (202), main memory (204), storage device (208), input device (210), output device (212) and communication interface (214). Processor (202) may include a processor, microprocessor, or processing logic that may interpret and execute instructions. Main memory (204) may include any dynamic storage device that may store information and instructions for execution by processor. Storage device may include a magnetic and/or optical recording medium and its corresponding drive. Input device may include a mechanism that permits an operator to input information to the device, such as a keyboard, a mouse, a pen, voice recognition and/or biometric mechanisms, etc. Output device (212) may include a mechanism that outputs information to the operator, including a display device, a printer device, a speaker device, etc. Communication interface (214) may include any transceiver-like mechanism that enables the device to communicate with other devices and/or systems. The device, consistent with principles of the invention, may perform certain operations. The device may perform these operations in response to processor executing machine readable instructions contained in a device-readable medium, such as memory. A device-readable medium may be defined as a physical or logical memory device and/or carrier wave. Machine readable instructions may be read into memory from another device-

readable medium, such as data storage device, or from another device via communication interface. The machine readable instructions contained in a memory may cause the processor to perform processes that will be described later. Alternatively, hardwired circuitry may be used in place of or in combination with machine readable instructions to implement processes consistent with principles of the invention.

Main memory (204) of the system further comprising secure memory location and non-transitory device-readable memory. The said secure memory location and said non-transitory device-readable memory having means for receiving machine readable flash via a network; disassembling said machine readable flash into machine readable instruction; locating a portion of the machine readable instruction making a network request associated with the machine readable flash; said secure memory location and said non-transitory device-readable memory whilst locating a portion of the machine readable instruction further having means for examining stack and trace constants of the machine readable instructions to locate a function; determining if said function is associated with making network request associated with machine readable flash; examining machine readable instructions to determine number of arguments for said function whilst said function is making a network request for machine readable flash; rewriting portion of machine readable instructions making the network request to redirect network communication associated with machine readable flash to secure memory location. The said secure memory location and said non-transitory device-readable memory whilst rewriting portion of the machine readable instructions further having means for replacing function invocation in the machine readable instructions with a rewriting function to redirect before invoking the function, the network communication associated with the machine readable flash to the secure memory location to prevent any modification in the machine readable flash, re-writing itself back to the original flash file at the execution level to assert originality, and providing secure communication of machine readable flash via network to a client device.

The at least one non-transitory device-readable memory stores executable instructions for securing delivery of machine readable flash over a network by said non-transitory device-readable memory comprising instructions. The said instructions executed by a processor, cause the processor; to determine whether an object of machine readable

instruction is of a certain class, to rewrite arguments of said machine readable instruction, to determine whether an application class of the machine readable instruction implements one or more actions that are unrelated to the network, to inject a machine readable instruction sequence that replaces a statement in the machine readable instruction when said machine readable instruction implements one or more actions that are unrelated to the network, to examine stack and trace constants of the machine readable instruction to locate an action related to making the network request associated with the machine readable flash, to determine a number of arguments for the action and to replace invocation of the action, in the machine readable instruction, with a rewriting function that redirects before invoking the action, the network communication associated with the flash content to a secure memory location.

The said instructions of said non-transitory device-readable memory further comprising instructions to inject a client-side process into the machine readable instruction. Further, said instructions to inject a client-side process into the machine readable instruction further comprising instructions to determine whether an object of the machine readable instruction is of a certain class; instructions to rewrite arguments of the machine readable instruction to redirect network communication of the object to the secure memory location when the object is of the certain class; instructions to determine whether an application class of the machine readable instruction implements an action unrelated to the network; and instructions to inject a machine readable instruction sequence that replaces a statement in the machine readable instruction when the application class implements the action unrelated to the network. The said machine readable instruction includes action codes comprising instructions defined on a virtual machine. The said non-transitory device-readable memory further comprising non-transitory readable memory device and said non-transitory readable memory device may be either a physical device or a virtual device.

Referring to FIG. 3, an embodiment of the method (300) of the invention is illustrated. Generally, the invention includes the steps for redirecting flash objects to a secure intermediate memory allocated segment according to an implementation consistent with principles of the invention. The methodology of FIG. 3 may begin when flash content is running on client. In one implementation, the methodology of FIG. 3 may be performed by one or more components within a network device. In another implementation, the

process may be performed by one or more components within another device or a group of devices separated from or including network device. As illustrated in FIG. 3, machine readable flash is first received by the network device (302). Thereafter, said machine readable flash is disassembled into machine readable instructions (304). Subsequently, a portion of the machine readable instructions is located by making a network request associated with machine readable flash (306) by examining stack and trace constants of machine readable instruction to locate a function (308); determining if said function is associated with making the network request associated with said machine readable flash (310); examining machine readable instruction to determine number of arguments for said function when said function is associated with making network request associated with machine readable flash (312); rewriting the portion of the machine readable instruction making the network request to redirect a network communication associated with machine readable flash to the secure memory location (314). Upon locating said portion of the machine readable instructions, a client side process is injected into the machine readable flash where the client side process rewrites the machine readable flash to redirect a network request for a flash object to the secure memory location when the flash object is of a certain class (320). The step of rewriting the machine readable flash consist of replacing a function invocation in the machine readable instruction with a rewriting function to redirect before invoking the function, the network communication associated with the machine readable flash to the secure memory location to prevent any further modification in the machine readable flash, re-writing itself back to the original flash file at the execution level to assert originality (316); and providing secure communication of the flash content, via the network, to a client device (318).

Upon injecting a client side process into the machine readable flash, flow analysis is performed on machine readable instruction and a stack of the machine readable instruction is inspected to locate an instruction parameter related to making the network request associated with the machine readable flash (322). Thereafter, it is followed by rewriting said machine readable instruction parameter to redirect the network communication associated with the machine readable flash to the secure location (324) and further said machine readable instruction parameter is replaced with the rewritten instruction parameter (326).

In short, the present invention provides secure delivery of machine readable flash over networks and mobile platforms by preventing manipulation and injection to mark machine readable flash for blocking purposes.

- 5 Unless the context requires otherwise or specifically stated to the contrary, integers, steps or elements of the invention recited herein as singular integers, steps or elements clearly encompass both singular and plural forms of the recited integers, steps or elements.
- 10 Throughout this specification, unless the context requires otherwise, the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated step or element or integer or group of steps or elements or integers, but not the exclusion of any other step or element or integer or group of steps, elements or integers. Thus, in the context of this specification, the term "comprising" is
- 15 used in an inclusive sense and thus should be understood as meaning "including principally, but not necessarily solely".

- It will be appreciated that the foregoing description has been given by way of illustrative example of the invention and that all such modifications and variations thereto as would
- 20 be apparent to persons of skill in the art are deemed to fall within the broad scope and ambit of the invention as herein set forth.

CLAIMS

1. A system (100) for secure delivery of flash content over networks and mobile platforms comprising:

5 at least one client (106) and server (102); and
 at least one network device (104) comprising at least one bus, processor (202), main memory (204), storage device (208), input device (210), output device (212) and communication interface (214)
 characterized in that

10 said main memory (204) further comprising at least one secure memory location and at least one non-transitory device-readable memory; said secure memory location and said non-transitory device-readable memory having means for

 receiving machine readable flash via a network;

15 disassembling said machine readable flash into machine readable instruction;

 locating a portion of the machine readable instruction making a network request associated with the machine readable flash;

 said secure memory location and said non-transitory device-readable memory whilst locating a portion of the machine readable instruction further

20 examining stack and trace constants of the machine readable instructions to locate a function;

 determining if said function is associated with making network request associated with machine readable flash;

25 examining machine readable instructions to determine number of arguments for said function whilst said function is making a network request for machine readable flash;

 rewriting portion of machine readable instructions making the network request to redirect network communication associated

30 with machine readable flash to secure memory location;

 said secure memory location and said non-transitory device-readable memory whilst rewriting portion of the machine readable instructions further

replacing function invocation in the machine readable instructions with a rewriting function to redirect before invoking the function, the network communication associated with the machine readable flash to the secure memory location to prevent any modification in the machine readable flash, re-writing itself back to the original flash file at the execution level to assert originality, and providing secure communication of machine readable flash via network to a client device.

2. A system (200) according to Claim 1, wherein the at least one non-transitory device-readable memory stores executable instructions for securing delivery of machine readable flash over a network by said non-transitory device-readable memory comprising instructions wherein said instructions

executed by a processor (202), cause the processor (202) to determine whether an object of machine readable instruction is of a certain class;

executed by said processor (202), cause the processor (202) to rewrite arguments of said machine readable instruction;

executed by said processor (202), cause the processor (202) to determine whether an application class, of the machine readable instruction implements one or more actions that are unrelated to the network;

executed by said processor (202), cause the processor (202) to inject a machine readable instruction sequence that replaces a statement in the machine readable instruction when said machine readable instruction implements one or more actions that are unrelated to the network;

executed by the processor (202), cause the processor (202) to examine stack and trace constants of the machine readable instruction to locate an action related to making the network request associated with the machine readable flash;

executed by the processor (202), cause the processor (202) to determine a number of arguments for the action; and

executed by the processor (202), cause the processor (202) to replace invocation of the action, in the machine readable instruction, with a

rewriting function that redirects before invoking the action, the network communication associated with the flash content to a secure memory location.

- 5 3. A system according to Claim 2, wherein said instructions of said non-transitory device-readable memory further comprising instructions to inject a client-side process into the machine readable instruction.
- 10 4. A system according to Claim 3, wherein said instructions of said non-transitory device-readable memory to inject a client-side process into the machine readable instruction further comprising:
 - instructions to determine whether an object of the machine readable instruction is of a certain class;
 - instructions to rewrite arguments of the machine readable instruction, to
 - 15 redirect network communication of the object to the secure memory location, when the object is of the certain class;
 - instructions to determine whether an application class, of the machine readable instruction implements an action unrelated to the network; and
 - instructions to inject a machine readable instruction sequence that
 - 20 replaces a statement in the machine readable instruction when the application class implements the action unrelated to the network.
- 25 5. A system according to Claim 1, wherein said machine readable instruction includes action codes comprising instructions defined on a virtual machine.
- 30 6. A system according to Claim 2, wherein said non-transitory device-readable memory further comprising non-transitory readable memory device.
7. A system according to Claim 6, wherein said non-transitory readable memory device may be either a physical device or a virtual device.
8. A method (300) for secure delivery of flash content over networks and mobile platforms, the method comprising steps of:
 - receiving machine readable flash by a network device (302);

disassembling said machine readable flash into machine readable instructions (304);

locating a portion of the machine readable instructions making a network request associated with machine readable flash (306) which includes

5 examining stack and trace constants of machine readable
instruction to locate a function (308);
determining if said function is associated with making the network
request associated with said machine readable flash (310);
examining machine readable instruction to determine number of
10 arguments for said function when said function is associated with
making network request associated with machine readable flash
(312);
rewriting the portion of the machine readable instruction making
the network request to redirect a network communication
15 associated with machine readable flash to the secure memory
location (314);

injecting a client side process into the machine readable flash where
the client side process rewrites the machine readable flash to redirect a
network request for a flash object to the secure memory location when
20 the flash object is of a certain class (320);

performing flow analysis on the machine readable instruction and
inspecting a stack of the machine readable instruction to locate an
instruction parameter related to making the network request associated
with the machine readable flash (322);

25 rewriting said machine readable instruction parameter to redirect the
network communication associated with the machine readable flash to the
secure location (324); and

replacing the machine readable instruction parameter with the rewritten
instruction parameter (326)

30 characterized in that
rewriting the portion of the machine readable instruction making the
network request to redirect a network communication associated with
executable content to the secure memory location (314) further comprises
steps of:

replacing a function invocation in the machine readable instruction with a rewriting function to redirect before invoking the function, the network communication associated with the machine readable flash to the secure memory location to prevent any further modification in the machine readable flash, re-writing itself back to the original flash file at the execution level to assert originality (316); and providing secure communication of the flash content, via the network, to a client device (318).

5

10