[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 03104964.8

[45] 授权公告日 2010 年 3 月 17 日

[11] 授权公告号 CN 100594484C

[22] 申请日 2003.3.4 [21] 申请号 03104964.8

[73] 专利权人 高振宇

地址 100044 北京市西外大街 142 号院内小楼

[72] 发明人 高振宇

[56] 参考文献

CN1269030A 2000.10.4

CN1271895A 2000.11.1

CN1372201A 2002.10.2

CN1170903A 1998.1.21

审查员 赵小宁

[74] 专利代理机构 北京北新智诚知识产权代理有限公司

代理人 赵郁军

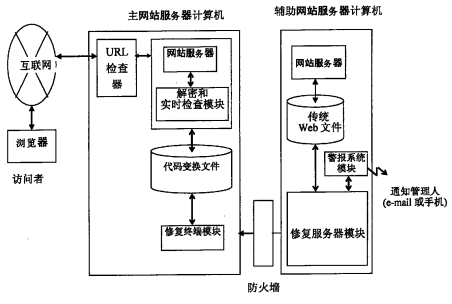
权利要求书 3 页 说明书 12 页 附图 4 页

[54] 发明名称

网站服务器系统

[57] 摘要

网站服务器系统包括彼此相连的主网站服务器计算机和辅助网站服务器计算机，在它们之间设有防火墙。主网站服务器计算机具有防止篡改、解密、可处理静态、动态 Web 文件、http 通信协议功能。在主网站服务器计算机内存储有由 Web 文件生成的第一代码变换文件；在辅助网站服务器计算机内存储有 Web 文件。在主网站服务器计算机内包含有一个具有检查、判断第一代码变换文件是否被篡改的主网站服务器。当第一代码变换文件被篡改时，辅助网站服务器计算机将其存储的 Web 文件进行处理生成第二代码变换文件，送至主网站服务器计算机中，更新、修复被篡改或删除的第一代码变换文件。主网站服务器再将第一代码变换文件转换复原成所述的 Web 文件送给访问者。



1、一种网站服务器系统，其特征在于：它包括主网站服务器计算机和辅助网站服务器计算机，所述主网站服务器计算机和辅助网站服务器计算机彼此之间相连，并且在所述主网站服务器计算机和辅助网站服务器计算机之间设有防火墙；

所述主网站服务器计算机具有防止篡改、解密、可处理静态 Web 文件、动态 Web 文件、http 通信协议以及支持动态网页、数据库、SSL 功能，在所述主网站服务器计算机内存储有由 Web 文件生成的第一代码变换文件；

在所述辅助网站服务器计算机内存储有 Web 文件；在所述辅助网站服务器计算机内包含有一个辅助网站服务器；

在所述主网站服务器计算机内包含有一个具有检查、判断所述第一代码变换文件是否被篡改的主网站服务器；

当所述主网站服务器计算机接收到访问者的请求时，所述主网站服务器对存储在所述主网站服务器计算机内的所述第一代码变换文件进行检查、判断其是否被篡改；当所述第一代码变换文件没有被篡改时，所述主网站服务器对所述第一代码变换文件进行处理并回送给 Web 访问者；

当检查出所述第一代码变换文件被篡改时，所述辅助网站服务器将存储在所述辅助网站服务器计算机记忆装置或与之相连的记忆装置中的所述 Web 文件进行处理生成第二代码变换文件，送至所述主网站服务器计算机的记忆装置中，更新、修复被篡改的所述第一代码变换文件，所述主网站服务器再将所述第一代码变换文件转换复原成所述的 Web 文件，将该复原后的所述 Web 文件送给访问者。

2、如权利要求 1 所述的网站服务器系统，其特征在于：

所述第一代码变换文件是由所述存储在主网站服务器计算机内的 Web 文件加密处理而生成的；

当所述第一代码变换文件没有被篡改时，所述主网站服务器对所述第一代码变换文件进行解密处理并回送给访问者；

当所述第一代码变换文件被篡改时，所述辅助网站服务器将存储在其记忆装置或与之相连的记忆装置中的所述 Web 文件进行加密处理生成所述第二代码变换文件，送至所述主网站服务器计算机的记忆装置中，更新、修复被篡改的所述第一代码变换文件，所述主网站服务器再将新的所述第一代码变换文件解密复原成所述的 Web 文件，将该复原后的所述 Web 文件送给访问者。

3、如权利要求 1 所述的网站服务器系统，其特征在于：

所述第一代码变换文件带有防止篡改的头信息，该头信息中包括有对所述存储在主网站服务器计算机内的所述 Web 文件进行认证而得到的认证子和文件的有关信息；

当所述主网站服务器计算机接收到访问者的请求时，所述主网站服务器从所述带有防止篡改的头信息的第一代码变换文件中把所述头信息分离，用该头信息中的认证子对所述存储在主网站服务器计算机内的所述 Web 文件进行实时认证检查处理；

所述主网站服务器通过实时认证检查处理判断所述第一代码变换文件是否被篡改；当所述第一代码变换文件没有被篡改时，所述主网站服务器将除去所述头信息的所述存储在主网站服务器计算机内的 Web 文件发送给访问者；

当检查出所述带有头信息的第一代码变换文件被篡改时，将存储在所述辅助网站服务器计算机记忆装置或与之相连的记忆装置中的所述 Web 文件进行认证处理生成带有防止篡改的所述头信息的第二代码变换文件，送至所述主网站服务器计算机，更新、修复被篡改的所述第一代码变换文件，所述主网站服务器再将新的所述第一代码变换文件转换复原成所述的 Web 文件，将该复原后的所述 Web 文件送给访问者。

4、如权利要求 1 所述的网站服务器系统，其特征在于：所述第一代码变换文件是由所述存储在主网站服务器计算机内的所述 Web 文件加密处理而生成的，在该第一代码变换文件中带有防止篡改的头信息，该头信息中包括有对所述存储在主网站服务器计算机内的 Web 文件进行认证而得到的认证子；

当所述主网站服务器计算机接收到访问者的请求时，所述主网站服务器从所述带有防止篡改的头信息的第一代码变换文件中把所述头信息分离，用该头信息中的认证子对所述存储在主网站服务器计算机内的 Web 文件进行实时认证检查处理；

所述主网站服务器通过实时认证检查处理判断所述第一代码变换文件是否被篡改；当所述第一代码变换文件没有被篡改时，所述主网站服务器将除去所述头信息并且解密复原成所述 Web 文件，将复原后的该 Web 文件发送给访问者；

当检查出所述带有头信息的第一代码变换文件被篡改时，将存储在所述辅助网站服务器计算机记忆装置或与之相连的记忆装置中的所述 Web 文件进行认证以及加密处理生成带有防止篡改的所述头信息的第二代码变换文件，送至所述主网站服务器计算机，更新、修复被篡改的所述第一代码变换文件，再由所述主网站服务器将新的所述第一代码变换文件除去所述头信息并且解密复原成所述的 Web 文件，将复原后的该

Web 文件送给访问者。

5、如权利要求 2 或 4 所述的网站服务器系统，其特征在于：所述第一代码变换文件是通过混沌加密算法生成的。

6、如权利要求 3 或 4 所述的网站服务器系统，其特征在于：所述第一代码变换文件头信息中包含的认证子是通过混沌认证和混沌加密处理生成的。

7、如权利要求 1~4 之一所述的网站服务器系统，其特征在于：在所述主网站服务器计算机内还包括有一个 URL 检查器，该 URL 检查器放置在所述主网站服务器的 URL 入口处；当接收到 URL 格式的请求时，该 URL 检查器将该 URL 格式的请求与存储在所述主网站服务器计算机的记忆装置中的非法 URL 模式库进行比较，如果发现与该库中保存的黑客模式或病毒模式一致，则自动封闭发出该 URL 格式请求的 IP，并拒绝其连接请求，防止前门攻击。

网站服务器系统

技术领域

本发明是关于互联网中网站服务器（Web server）计算机系统，具体地说，本发明是关于具有对外可信、自身安全特点的网络服务器计算机系统。

背景技术

网站服务器(Web server, http server)是构筑电子政务、电子银行、电子商务、网络服务等各种现代通信网络系统的最重要的基础平台之一。

第1代网站服务器是以处理静态网页为主。网站服务器推到互联网（Internet）世界后，引发了互联网的商业狂潮。其基本功能是，当得到来自浏览器的请求时，网站服务器将执行有关文件，并将结果或有关文件以网页的形式，依照http通信协议送回给浏览器。在此类网站服务器的存储器中，存储着html、HTML、TEXT、GIF、JPEG、图形、声音等静止的Web文件及可在浏览器侧运行的象 .exe这样的可执行的文件等Web文件。

为了进一步发展网上商店、网上银行、电子政府和各种网站，人们又发明了第2代网站服务器。即，在第1代网站服务器的基础上，又增添了支持动态网页和数据库，SSL等功能。例如，现在大约占全球市场2/3的Apache，占全球市场1/3的IIS。

但是，当今第2代网站服务器有着以下重大安全漏洞和重要问题:

最重大的问题是,几乎所有的Web文件,包括静态文件和动态文件,都是不加密的“平文文件（Plain Text）”。因为当今第2代网站服务器不能处理加密的Web文件,而且不提供篡改检查功能。黑客们知道这些重大安全漏洞的存在，并且知道如何利用这些安全漏洞去获取非法利益。包括政治利益，经济利益或个人利益。正是这些重大安全漏洞或缺陷吸引着黑客们不间断地攻击网站。

所以，第2代网站服务器表现出以下的各种问题:

1）不可信(No trust)

随时可能被篡改成他人的内容（网页）。于是会造成各种严重问题，如: 企业的网站会丧失对客人的信用，政府的网站会失信于民;

- 政治问题（例: 法轮功）;
- 经济问题（例: 汇率，股价被改）;
- 社会问题（例: 银行首页）;

. 国际问题（例：中美黑客大战）。

2）侵入内部数据库的窗口

. 高明的黑客可以进入网站服务器而窃取位于内侧的数据库的 IP，名称，口令（password）等信息!从而侵入数据库。

2002 年，2000 黑客出席的纽约黑客大会上的最热门技术。

3）http 病毒的传播媒介

这是在网站服务器与终端浏览器之间交叉感染的一种电脑病毒。

例：Nimda，Codered。

4）无法用防火墙等周边安全产品将其完全封闭保护

因为网站的主人希望外部的人来看自己的网站，所以必须在防火墙上留有通道(port)。

对网站服务器的攻击可分为：

1)前门攻击

通常使用 HTTP 协议，URL 和 80 端口，攻击 Web 的弱点。 攻击者包括黑客和网络病毒。防火墙不能防御此类攻击。

2)后门攻击

通常情况下,黑客首先用黑客工具等攻破 Web 服务器的口令;然后通过 FTP,Telnet 等侵入服务器;最后,黑客可以做任何他想做的事情,如涂改网页偷窃文件/数据等。

38%的被访者说他们的网站在过去的一年中被攻破。70%的组织报告遭受在线涂改。从事涂改的黑客用自己的文字或令人厌恶的图片替代网站的首页。

为了解决第 2 代网站服务器的网页易被黑客篡改的问题，市场上虽然出现了两类产品，显然无法解决全部问题。他们的技术特点及不足点如下：

●文件扫描型（File scanner 型）

无 Web 功能;

无“抗偷窃”功能；无法保护内部数据库服务器（DB server）;

未考虑防御 http 病毒的问题;

无法实现“0 秒恢复”;

大幅度增加 CPU 负荷。

●HD I/O 控制型

无 Web 功能;

无“抗偷窃”功能；无法保护内部数据库服务器（DB server）;

未考虑防御 http 病毒的问题;

无法实现不中断保护。

发明内容

鉴于上述原因，本发明的目的是提供一种可信与安全的网站服务器系统。该网站服务器是在现有网站服务器的基础上，增加“可信”和“安全”的功能，具有以下主要功能：

1)可信 （Trust）：

提供干净的和可信的(clear and trust)网页，没有黑客的篡改，没有病毒的污染。

2)安全（Security），抗击攻击：

抗击黑客、恐怖分子的应用层攻击和通信层攻击。

抗击 http 病毒攻击：Nimda, CodeRed etc。

防止偷窃及盗听：

秘密数据；收费信息；数据库的 ID, IP，姓名（Name），口令（password）等。

程序自身：电子政务，电子银行，电子商务，ERP 等。

3)静态网页（Static Pagers）(html, jpg,gif,wav,mp3,etc.)。

4)动态网页（Dynamic Pager） (CGI, Perl, php,java, etc.)。

5)数据库（DB）(mysql, SQL, Oracle, etc.)。

6)SSL 等。

为实现上述目的，本发明采用以下技术方案：一种网站服务器系统，它包括主网站服务器计算机和辅助网站服务器计算机，所述主网站服务器计算机和辅助网站服务器计算机彼此之间相连，并且在所述主网站服务器计算机和辅助网站服务器计算机之间设有防火墙；

所述主网站服务器计算机具有防止篡改、解密、可处理静态 Web 文件、动态 Web 文件、http 通信协议以及支持动态网页、数据库、SSL 功能，在所述主网站服务器计算机内存储有由 Web 文件生成的第一代码变换文件；

在所述辅助网站服务器计算机内存储有 Web 文件；在所述辅助网站服务器计算机内包含有一个辅助网站服务器；

在所述主网站服务器计算机内包含有一个具有检查、判断所述第一代码变换文件是否被篡改的主网站服务器；

当所述主网站服务器计算机接收到访问者的请求时，所述主网站服务器对存储在所述主网站服务器计算机内的所述第一代码变换文件进行检查、判断其是否被篡改；当所述第一代码变换文件没有被篡改时，所述主网站服务器对所述第一代码变换文件进行处理并回送给 Web 访问者；

当检查出所述第一代码变换文件被篡改时，所述辅助网站服务器将

存储在所述辅助网站服务器计算机记忆装置或与之相连的记忆装置中的所述 Web 文件进行处理生成第二代码变换文件，送至所述主网站服务器计算机的记忆装置中，更新、修复被篡改的所述第一代码变换文件，所述主网站服务器再将所述第一代码变换文件转换复原成所述的 Web 文件，将该复原后的所述 Web 文件送给访问者。

在本发明的具体实施例中，本发明共提供了三种结构的可信与安全的网站服务器。

在第一种结构的可信与安全网站服务器中，所述第一代码变换文件是由所述存储在主网站服务器计算机内的 Web 文件加密处理而生成的；

当所述第一代码变换文件没有被篡改时，主网站服务器对所述第一代码变换文件进行解密处理并回送给访问者；

当所述第一代码变换文件被篡改时，所述辅助网站服务器计算机将其记忆装置或与之相连的记忆装置中的所述 Web 文件进行加密处理生成第二代码变换文件，送至所述主网站服务器计算机的记忆装置中，更新、修复被篡改的所述第一代码变换文件，主网站服务器计算机再将新的所述第一代码变换文件解密复原成所述的 Web 文件，将该复原后的 Web 文件送给访问者。

在第二种结构的可信与安全网站服务器中，所述第一代码变换文件带有防止篡改的头信息，该头信息中包括有对所述存储在主网站服务器计算机内的 Web 文件进行认证而得到的认证子；

当所述主网站服务器计算机接收到访问者的请求时，主网站服务器从所述带有防止篡改的头信息的第一代码变换文件中把所述头信息分离，用该头信息中的认证子对所述存储在主网站服务器计算机内的 Web 文件进行实时认证检查处理；

所述主网站服务器通过实时认证检查处理判断所述第一代码变换文件是否被篡改；当所述第一代码变换文件没有被篡改时，主网站服务器将除去头信息的所述存储在主网站服务器计算机内的 Web 文件发送给访问者；

当检查出所述带有头信息的第一代码变换文件被篡改时，将存储在所述辅助网站服务器计算机记忆装置或与之相连的记忆装置中的 Web 文件进行认证处理生成带有防止篡改的头信息和其他有关信息的第二代码变换文件，送至所述主网站服务器计算机，更新、修复被篡改的所述第一代码变换文件，主网站服务器再将新的所述第一代码变换文件转换复原成所述的 Web 文件，将复原后的该 Web 文件送给访问者。

在第三种结构的可信与安全的网站服务器中，所述第一代码变换文件是由所述存储在主网站服务器计算机内的 Web 文件加密处理而生成

的，在该第一代码变换文件中带有防止篡改的头信息，该头信息中包括有对所述存储在主网站服务器计算机内的 Web 文件进行认证而得到的认证子；

当所述主网站服务器计算机接收到访问者的请求时，主网站服务器从所述带有防止篡改的头信息的第一代码变换文件中把所述头信息分离，用该头信息中的认证子对所述存储在主网站服务器计算机内的 Web 文件进行实时认证检查处理；

所述主网站服务器通过实时认证检查处理判断所述第一代码变换文件是否被篡改；当所述第一代码变换文件没有被篡改时，主网站服务器将除去头信息并且高速解密后的 Web 文件发送给访问者；

当检查出所述带有头信息的第一代码变换文件被篡改时，将存储在所述辅助网站服务器计算机记忆装置或与之相连的记忆装置中的 Web 文件进行认证以及加密处理生成带有防止篡改的头信息的第二代码变换文件，送至所述主网站服务器计算机，更新、修复被篡改的所述第一代码变换文件，然后由主网站服务器将新的所述第一代码变换文件除去头信息并且高速解密复原成所述的 Web 文件，将复原后的该 Web 文件送给访问者。

本发明开发的网站服务器,将会有以下效果:

①即使非法入侵者侵入了本发明提供的的网站服务器，他们无法对 Web 文件做任何有意义的篡改，无法偷盗保密信息或程序。

②即使遭受到黑客的篡改，被篡改的 Web 文件不能向访问者送出。即：访问者永远看不到被篡改的网页。

③被篡改的 Web 文件可以被自动恢复。

④进行 Web 网页的日常更新时，不用停止防止系统被篡改的功能。

⑤为了不同的操作系统（OS）间容易移植，本发明篡改防止系统构筑在系统的应用层上。

⑥对于已经使用的既存网站，容易导入本发明公开的网站服务器系统。

为了解决现有技术存在的问题，实现本发明的发明目的，本发明提出了一种具有对外可信、自身安全、包括当今第二代网站服务器功能在内的网站服务器系统。上述的 “对外可信”是指：当本发明公开的网站服务器接收到来自访问者的 URL 请求时，可防止遭黑客篡改或被电脑病毒污染的网页被通过 http 等通信协议回送给访问者;上述的“自身安全”是指抗击攻击，包括：黑客的应用层攻击，通信层攻击及 http 电脑病毒攻击等的攻击；前述“自身安全”还包括防止放置在网站服务器硬盘存

贮器中的秘密数据和应用程序被入侵黑客偷窃及盗听；前述第二代网站服务器功能包括类似 Apache，IIS 的支持处理静态文件，动态文件及 http 通信协议，SSL 等的功能。

本发明提出了具有以下特征的网站服务器系统：（1）放置由 Web 文件被加密处理而生成的“第一、第二代码变换文件”的，具有防止篡改、解密功能及可处理静态 Web 文件、动态 Web 文件、http 通信协议及第二代 Web server 功能的主网站服务器计算机；（2）与主网站服务器计算机连接的，放置前述 Web 文件的辅助网站服务器计算机；（3）当接到访问者的要求时，主网站服务器计算机中的网站服务器对“第一代码变换文件”进行检查，在判断为没被篡改的情况下，将“第一代码变换文件”解密并回送给访问者；（4）在检出“第一代码变换文件”被非法篡改时，将辅助网站服务器计算机的记忆装置或与之连接的记忆装置中放置的 Web 文件进行加密处理而成的“第二代码变换文件”，送至主网站服务器计算机的记忆装置中，更新，恢复被篡改的 Web 文件。

本发明还提出了具有以下特征的网站服务器系统：（1）放置带有防止篡改的头信息---该头信息中包括有对 Web 文件进行认证（authentication）而得的认证子（简称 MAC，全称 Message Authentication Cord)---以及文件大小，日期等有关信息的“第一代码变换文件”的，具有防止篡改功能的主网站服务器计算机；（2）与具有防止篡改功能的主网站服务器计算机相连的，放有 Web 文件的辅助网站服务器计算机；（3）当接到访问者的要求时，主网站服务器计算机中的网站服务器，从带有防止篡改的头信息的“第一代码变换文件”中把该头信息分离，用该头信息中 MAC 对 Web 文件进行对照检查的实时检查处理（real time check）；（4）通过实时检查处理判断 Web 文件没被篡改时，主网站服务器将除去头信息的 Web 文件发送给访问者；（5）当检出带有防止篡改的头信息的“第一代码变换文件”被篡改时，将辅助网站服务器计算机的记忆装置或与之连接的记忆装置中放置的 Web 文件进行认证处理，以得到带有防止篡改的头信息的“第二代码变换文件”，并将该“第二代码变换文件”送至具有防止篡改功能的主网站服务器计算机，以更新，修复被篡改的“第一代码变换文件”。

本发明还提出了具有以下特征的网站服务器系统：包括了（1）放置带有防止篡改的头信息---该头信息中包括有对 Web 文件进行认证（authentication）而得的认证子（简称 MAC，全称 Message Authentication Cord)---的，并由 Web 文件加密处理而成的“第一代码变换文件”的，具有防止篡改、解密机能、可处理静态 Web 文件、动态 Web file、http 通信协议以及第二代网站服务器功能的主网站服务

器计算机；（2）与具有防止篡改、解密功能、可处理静态 Web 文件、动态 Web 文件、http 通信协议及第二代网站服务器功能的主网站服务器计算机相连的，放有 Web 文件的辅助网站服务器计算机；（3）当接到访问者的要求时，主网站服务器计算机中的网站服务器，从带有防止篡改的头信息的“第一代码变换文件”中把该头信息分离，用该头信息中的 MAC 对 Web 文件进行对照检查的实时检查处理(real time check)；（4）通过实时检查处理判断 Web 文件没被篡改时，主网站服务器将除去头信息的 Web 文件发送给访问者；（5）当检出带有防止篡改的头信息的“第一代码变换文件”被篡改时，将辅助网站服务器计算机的记忆装置或与之连接的记忆装置中放置的 Web 文件进行认证以及加密处理，以得到带有防止篡改的头信息的“第二代码变换文件”，并将该“第二代码变换文件”送至具有防止篡改功能的主网站服务器计算机，以更新，修复被篡改的“第一代码变换文件”。

本发明提供的网站服务器系统还具有以下特征：当接收到 URL 格式的请求时，将接收到的 URL 格式的请求与放置在计算机的记忆装置中的”非法 URL 库”做比较，如果发现与该库中保存的”黑客模式”或”病毒模式”一致则自动封闭发出该 URL 的 IP；拒绝其连续请求，防止前门攻击的手段。

本发明提供的网站服务器系统还具有以下特征：可自动地判断放置在计算机的记忆装置中的 Web 文件，何为“合法更新”，何为电脑黑客的“非法篡改”，以实现对网站服务器的“不中断保护”。

本发明采用的实时检查处理（real time check）是基于消息认证技术(Chaos Message Authentication Technology)，具有防止网页被篡改的功能。

本发明采用的加密处理可以使用基于混沌理论(Chaos theory)的加密法，前述的认证(authentication)处理可以使用基于混沌理论的消息认证处理（ Massage Authentication Technology ）。

本发明提供的网站服务器系统具有以下的优点：

- 继承目前网站服务器的功能，包括：
  - 静态网页 Static Pagers *(html, jpg, gif, wav, mp3, etc.)*；
  - 动态网页 Dynamic Pager: *(CGI, Perl, php, java, etc.)*；
  - 数据库：DB *(mysql, SQL, Oracle, etc.)*；
  - SSL 等。
- 容易与目前网站服务器共用，提升其可信及安全的功能。
- Web 文件的认证及超高速代码变换：从原

理上杜绝了网页(home page)被篡改，被偷窃及被 Web 病毒污染的问

题。

❑0 秒恢复: 上网的浏览者在任何时候都不能从网站上看到被非法改变的网页。 即使黑客更换,删除了 Web 文件,该系统可以在 Web 文件被送出的瞬间,自动恢复。

❑无间断保护: 24 小时自动无间断保护。即使需要更新网页时也不必停止该系统, 可自动识别网页的非法篡改与正常更新。

❑防止 Web 病毒: Web 病毒(http 病毒)是一种利用 http 通信协议传播的特殊的电脑病毒。

本发明提供的第 3 代网站服务器系统(3GWeb)既可以防止其污染网页,也可以阻断其连续攻击。例如: Code Red, Nimda。

❑防止多种网络攻击: 诸如: Overflow 攻击, http DDoS 攻击, SQL Injection 攻击等。

❑拒绝执行非法程序: 诸如: Trojan Horses 攻击。

❑监测警报: 如果万一 Web 服务器不能正常工作,立刻向管理员发出警报。

❑最尖端安全技术: 使用混沌安全技术(Chaos Security Technology)。

❑支持多种安全产品: SSL, VPN, Firewall 等。

❑IE, Netscape 等各种浏览器无须做任何修正。 Web 服务器反应速度高。

使用本发明提供的网站服务器系统,从高速性方面来看,从浏览器的请求来到的瞬间,一瞬间即可完成认证检查和解密;与通常的第二代网站服务器相比反应速度几乎不变。

对于大型网站系统来说: (1)不增加网站服务器的负担。(2)检查和修复的速度不受网站系统的规模(文件数)大小影响。本发明对浏览器无影响。IE, Netscape 托从前的浏览器照样能使用。本发明提供的第 3 代网站服务器系统,具有动态的修复功能。发现篡改,会自动地高速修复文件。还有,设有自动警报机能。发现篡改,会自动通知系统管理人员。再者,容易植入现有的网站系统,不影响既存的网页编辑系统。

在本发明中,实现了(1)即使发生了篡改的行为,被篡改的 Web 文件也不会向外部 (网站访问者)送出,(2)即使有黑客的侵入,由于 Web 文件是被加密的,黑客不能进行有意义的篡改,更不能从中偷盗机密信息和系统程序等。再者,使用本发明,现在的网站(已经开设网页的 Web 系统)无需作全面的改写即可容易导入。特别是由于使用 G1 混沌加密算法和 Chaos MAM 混沌认证技术,使得本发明更具有高处理速度和高的安全性。

附图说明

图 1 为本发明的概念统构图。

图 2 本发明的消息认证技术原理说明图。

图 3 本发明的加密文件的构造的说明图。

图 4 为第二代网站服务器的构造的说明图。

图 5 为本发明的追加了实时检查（real time check）模块的网站服务器的构造的说明图。

图 6 为实时检查（real time check）模块的原理的说明图。

图 7 是本发明的第三代网站服务器概念的系统构成图。

具体实施方式

下面结合附图对本发明进行说明。

图 1 是本发明的系统全体的概念图。在本发明，对 Web 文件的全体进行认证处理(authentication)。当通过认证检查后知道 Web 文件被篡改时，不将该 Web 文件送出。同时会通知系统管理人员。当然，系统也会留有记录履历（log）。

消息认证(Message Authentication)处理的原理就象图 2 所示的那样，在送信侧，将消息 M 和密钥输入消息认证程序，生成认证子（MAC，Message Authentication Code）。然后，将此消息和认证子 MAC 送信。在收信侧，用接收到的消息 M′（由于有被篡改的可能性，不一定等于 M）和事先保有的密钥，生成新认证子（MAC′）。检查 MAC 和 MAC′，如果相等，则消息 M 的正当性被证明。若不相等则判断一定有过篡改。

图 3 现示了本发明的“第一代码变换文件”的构造。在被附加的头信息中，包括有文件的 MAC，尺寸，日期，属性，保存场所等的信息。在本发明的系统中采用的混沌加密算法(Chaos Encryption)及根据混沌理论的混沌消息认证(Chaos Authentication)技术。然而，使用其他的加密方法和消息认证技术在原理上也是可能的。

下面，对本发明的具有实时检查（real time check）功能的网站服务器的原理加以说明。众所周知，网站服务器的主要的工作，就是将被顾客请求的首页等 Web 文件送向访问者的 Web 浏览器。几乎所有的情况下，被请求的 Web 文件是放置在硬碟机中。网站服务器会依照来自浏览器的请求将 Web 文件找出，处理后，用 http 通信协议送还给发出请求的终端浏览器。

当前的网站服务器的原理通常如图 4 所示。即：

1）读入环境变量等的一些初期化处理；

2）用 http 通信协议接收来自 Web 浏览器的请求。该请求符合国际通用的 URL 格式；

3）必需的处理后，从硬碟机中读入被请求的文件;

4）将该被请求的文件，再通过 http 通信协议向 Web 浏览器送回。

在本发明中,如同图 5 所示，在将 Web 文件从硬碟机读入电脑内存的开放文件（Openfile）模块，与送信模块之间，新插入实时检查（real time check）模块，使之构成网页防止篡改系统的引擎。

图 6 显示了这个实时检查（real time check）模块的原理。在实时检查（real time check）模块中，首先根据请求信息，将收藏在硬碟机上的，被加密的，并且附有“防止篡改头信息”的（含有 MAC 等信息）文件读入电脑内存。

使用消息认证技术（massage authentication technology） 去检查该文件是否被篡改过; 如果没被篡改，则在一瞬间，切除掉“防止篡改头信息”的部分，并解密(Decryption)剩余的正文部分，再经送信模块回送给访问者的浏览器。

如果有被篡改的情况,向辅助网站服务器电脑中的“修复服务程序”发出修复要求。“修复服务程序”将对由“请求信息”指定的在辅助网站服务器电脑的目录里放置的原始文件进行加密,进而使用消息认证处理（massage authentication technology）生成 MAC，再将该 MAC 和该文件的尺寸，日期，时间，等属性的信息一起编入到“防止篡改头信息”中，再将该“防止篡改头信息”附加在该文件上。这个新文件被送给主网站服务器电脑。于是主网站服务器电脑中的被篡改的文件被更新（或被修复）。进而，这个更新的文件发回给浏览器。

在本发明的系统中，被篡改的文件，在被送信前，一定要经“消息认证”检查，并会被检出。所以从原理上，被篡改过的文件是不可能被送回给访问者的。

本发明在网站服务器系统中首先使用实时检查处理（real time check）技术。即本发明的防止篡改网站服务器，仅对被请求的文件，并且，仅当该文件被向外发送前进行检查，所以几乎不增加电脑 CPU 的负担。

为了实现真正实用的实时检查处理（real time check），选用高速的加密算法和高速且强力的认证技术是必需的。在这里，我们使用了世界高速的 GCC 或 G1 混沌加密(Chaos Encryption)算法和 MAM 混沌认证技术(Chaos Authentication Technology),实现了最高水准的第 3 代网站服务器系统。

为了防止黑客的前门攻击，在本发明中，首次设计了基于网站服务器的 URL 检查器。该 URL 检查器装在网站服务器的 URL 入口处。其原理是:

当接收到URL格式的“请求”时,从该“请求”的信息中抽出IP,与预置在计算机的记忆装置上的“IP控制表”对照检查。如果该表中有该IP,则拒绝该IP的请求,仅向发出该“请求”的计算机回送错误信息,不做其他的服务。若无此IP,则将该IP再与”非法URL库”做比较,如果与该库中保存的”黑客模式”或”病毒模式”一致则自动地将这个IP登入“IP控制表”,封闭发出该URL的IP,拒绝来自该IP的计算机的连续请求。

使用GCC或G1混沌加密法和ChaosMAM混沌认证技术来说明本发明的实施例。首先,简单地说明混沌加密法。现在设平文P,混沌加密函数G,密文C,密钥K,

C = G(K , P)

则平文P可被加密为密文C。把密文C解密的时候,使用混沌加密函数逆函数 G-1 和密钥K,则:

P = G-1(K , C)

可获得平文P。在这里平文P的长度自由。密钥K的长度是可变长,从8到2048位元。

本发明主要包括:主网站服务器和编码器/解码器模块和修复服务器和修复终端和警报系统,RUL检查器等部分。在主网站服务器里包括有第二代网站服务器的全部功能(例如,Apache)以及解码器功能,在编码器/解编码器模块中,有加密,生成MAC,头信息等功能的编码器部分和,含具有实时检查处理(real time check)等功能的解码器部分,在修复服务器里加有编码器的功能。

包含网页的HTML文件在内的Web文件放置在 辅助网站服务器 电脑的存储器上。通过修复服务器,对Web文件用GCC或G1混沌加密法加密,用ChaosMAM生成MAC,并将含有文件尺寸,日期, MAC等的头信息部分追加在该文件。进行所谓编码,并发送给外侧的主网站服务器中的修复终端。

修复终端,将收到的被编码处理后的Web文件放置在修复服务器指示的场所。

当从网路得到访问者的请求时,首先在URL过滤器中进行URL检查,如果发现是黑客攻击或是http病毒攻击,则封闭发出该URL的IP,拒绝其请求。如果通过URL检查,则:

主网站服务器中的具有防止篡改功能的Web server,从被编码的Web 文件的头信息部分中将MAC等信息取出;进行认证检查,当检查通过时,将头信息部分切除,并解密,(所谓解编码操作),再将复原的Web 文件送出给访问者。

如果在认证检查中被判断为被篡改时，修复终端将会向辅助网站服务器中的修复服务器发出修复请求，修复服务器依照修复请求，取出指定的文件，进行编码处理后，送出给主网站服务器。完成所谓的修复。同时，通知报警服务器，报警服务器将会把“非法侵入”通知系统管理人员。

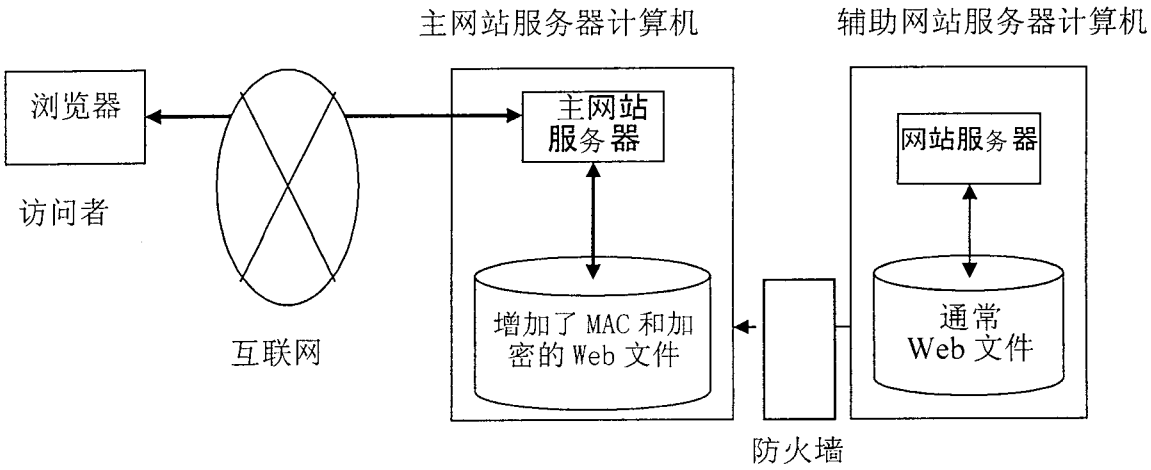

主网站服务器计算机
辅助网站服务器计算机
浏览器
访问者
互联网
主网站
服务器
增加了 MAC 和加
密的 Web 文件
网站服务器
通常
Web 文件
防火墙

图 1

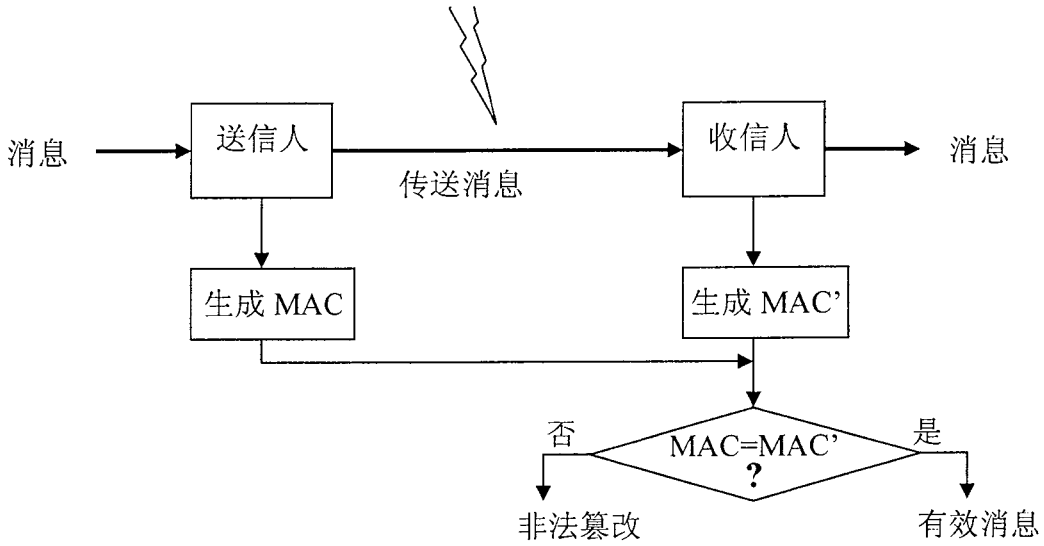

消息
送信人
传送消息
收信人
消息
生成 MAC
生成 MAC'
否
MAC=MAC'
?
是
非法篡改
有效消息

图 2

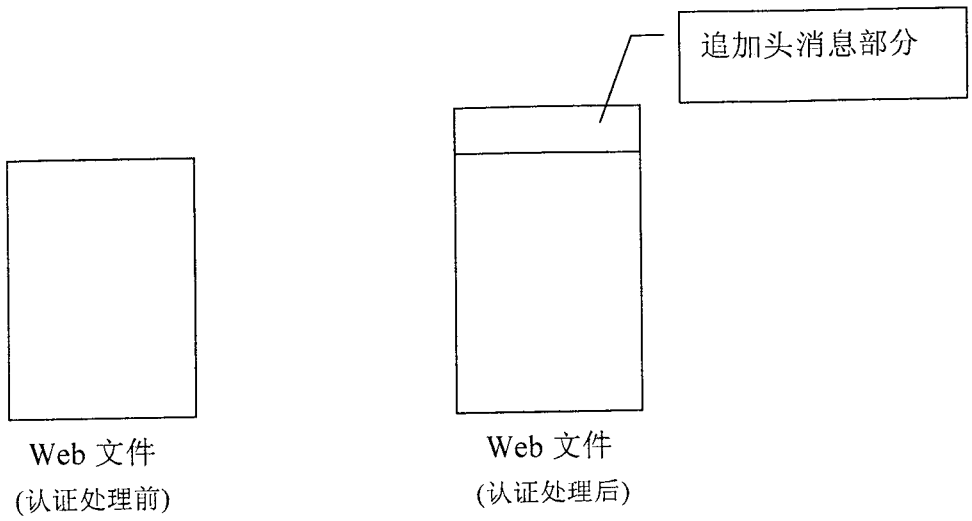

追加头消息部分
Web 文件
(认证处理前)
Web 文件
(认证处理后)

图 3

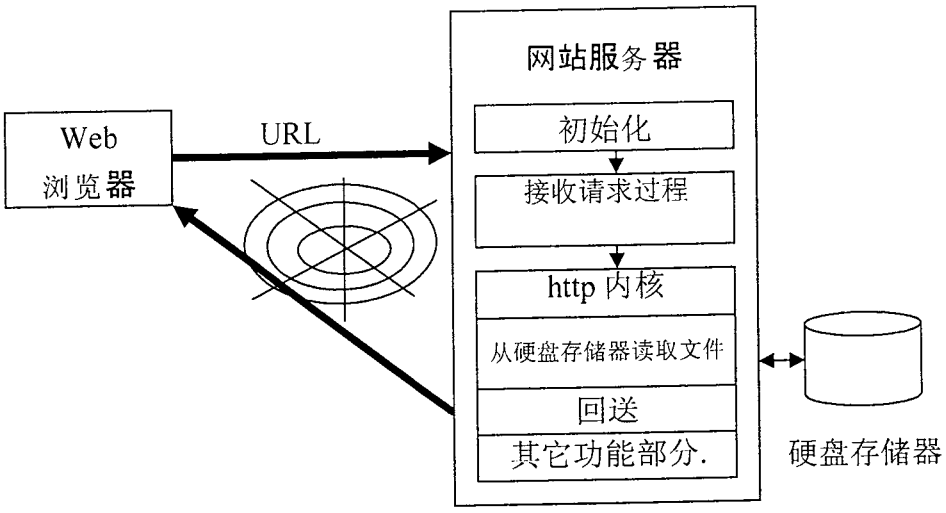

网站服务器
Web
浏览器
URL
初始化
接收请求过程
http 内核
从硬盘存储器读取文件
回送
其它功能部分.
硬盘存储器

图 4

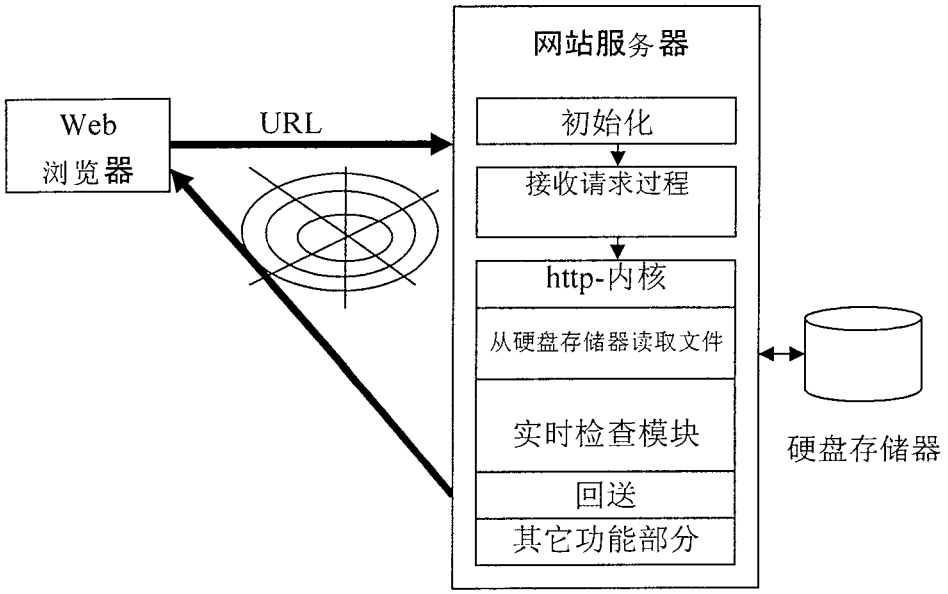

网站服务器
Web
浏览器
URL
初始化
接收请求过程
http-内核
从硬盘存储器读取文件
实时检查模块
回送
其它功能部分
硬盘存储器

图 5

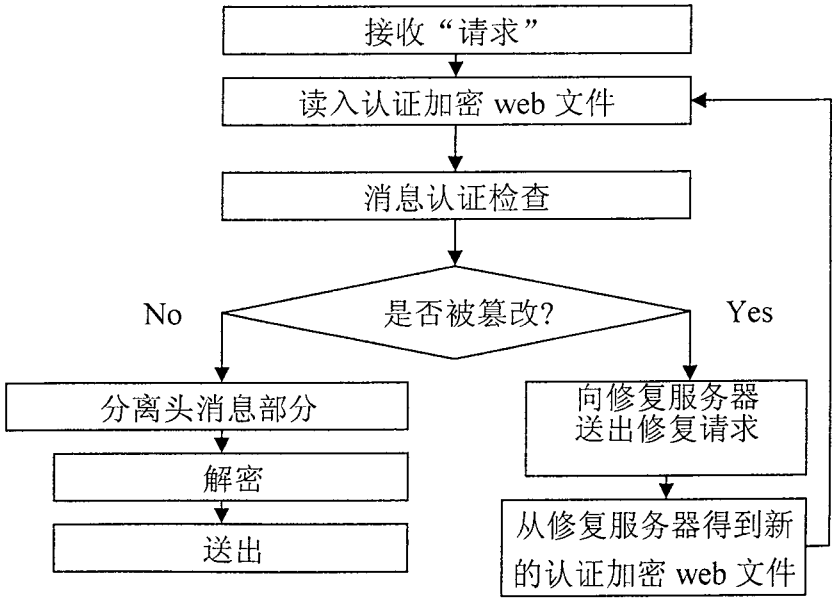

接收“请求”
读入认证加密 web 文件
消息认证检查
No
是否被篡改?
Yes
分离头消息部分
解密
送出
向修复服务器
送出修复请求
从修复服务器得到新
的认证加密 web 文件

图 6

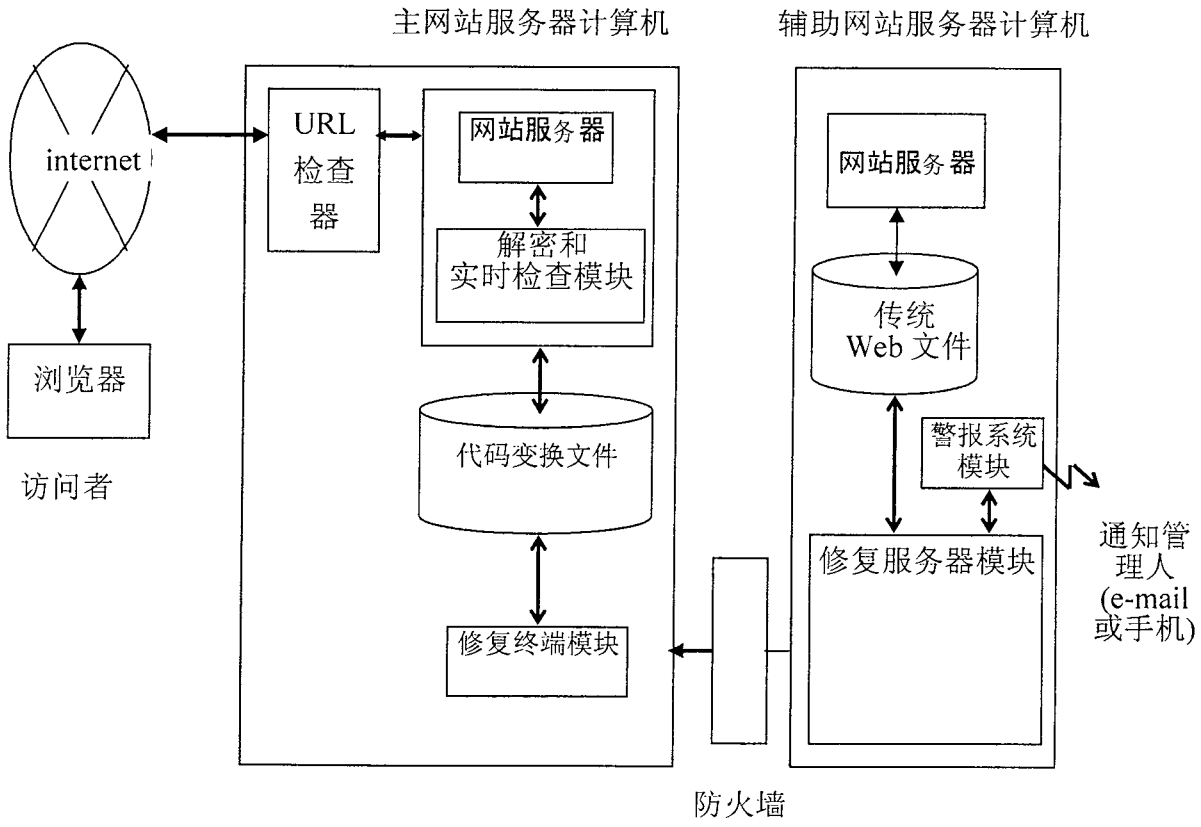

主网站服务器计算机
辅助网站服务器计算机
internet
URL
检查
器
网站服务器
解密和
实时检查模块
代码变换文件
修复终端模块
网站服务器
传统
Web 文件
警报系统
模块
修复服务器模块
浏览器
访问者
通知管
理人
(e-mail
或手机)
防火墙

图 7