

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(43) 国际公布日:
2002年3月28日(28.03.02)

PCT

(10) 国际公布号:
WO 02/25860 A1

- (51) 国际分类号⁷: H04L 9/00
- (21) 国际申请号: PCT/CN01/01401
- (22) 国际申请日: 2001年9月17日(17.09.01)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权: 00124551.1 2000年9月20日(20.09.00) CN
- (71)(72) 发明人/申请人: 慈孟夫(CI, Mengfu) [CN/CN]; 中国湖南省长沙市新开铺路39号, Hunan 410009 (CN).
- (74) 代理人: 广州专利事务所(GUANGZHOU PATENT AGENCY); 中国广东省广州市仓边路87号四楼, Guangdong 510030 (CN).
- (81) 指定国(国家): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ,
- LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW
- (84) 指定国(地区): ARIPO专利(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI专利(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

根据细则4.17的声明:

- 关于申请人在国际申请日有权申请并被授予专利(细则4.17(ii))对所有指定国
- 发明人资格(细则4.17(iv))仅对美国

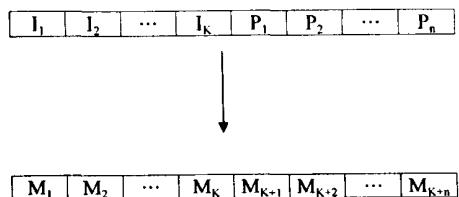
本国际公布:

- 包括国际检索报告。

所引用双字母代码和其它缩写符号, 请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(54) Title: THE DYNAMIC IDENTIFICATION METHOD WITHOUT IDENTIFICATION CODE

(54) 发明名称: 无标识全动态认证方法



WO 02/25860 A1

(57) Abstract: The invention provides a dynamic identification method that has no identification code. A User terminal transfers the user's original identification code and ID codes which have been encrypted to the server, and the server confirms the user's ID after decrypting them. The method provided by the invention dynamic encrypts user's original identifier and ID codes, so when user ID is identified every time, because the same user comes to each different results every encryption, there isn't a static identification or character to be distinguished. It makes an attacker have no way to trace, record and analyse a user's ID information. And it makes an attacker who wants to disclose one user's ID information have to disclose all users'. Therefore, the method brings us much more security than before.

[见续页]



(57) 摘要

本发明公开了一种无标识全动态认证法，用户终端将用户的原始认证标识码和认证码进行动态加密后传送至服务器，服务器对动态的认证标识码和认证码解密后进行用户身份确认。本发明采用的认证方法，由于对认证标识码和认证码均进行一动态加密，故用户每次进行身份认证时，由于每次加密所得的结果均不相同，没有一个静态标识和特征可供辨识，使攻击者无法对用户的认证信息进行跟踪、记录、分析。实际上造成攻击者破解某一用户的变化规律变成了破解所有用户的变化规律，具有更高的安全性。

无标识全动态认证方法

本发明所属技术领域

本实用新型涉及一种无标识全动态认证方法，属于信息安全领域。

在本发明之前的现有技术

5 计算机网络用户认证普遍采用静态的标识码和口令相结合进行用户身份的确
认，上述的标识码一般指用户名、序号等。口令为用户设定的密码。由于这种身
份认证方法所采用的静态标识码和口令从用户端传送至服务器进行身份认证时，
没有一个动态的变化，故在用户端和服务器之间的认证信息传送过程中，一旦被
攻击者截获，就可以冒充授权用户进行攻击。鉴于上述静态认证方法存在的缺陷，
10 现发展形成了一种新的用户认证方法，其在上述认证方法的基础上，把静态的口
令改为动态口令，即静态标识码+动态口令。上述这类认证方法，已有多种产品
推出市场，例如美国的数据安全公司(RAS)推出的 Dynamic ID 动态口令卡使用“密
钥一时间(事件)”双因素，依不同的时间自动产生动态口令进行认证。其实，任
何一个使用动态口令进行认证的用户，他的动态口令的变化均依照某种规律，攻
15 击者可根据静态标识码不变的弱点进行跟踪截获分析，只要截获了足够的信息，
就有可能破解动态口令的变化规律，从而进行冒充授权用户攻击。

本发明的目的

本发明提供一种令攻击者无法进行跟踪分析的认证方法。

本发明的技术方案

20 本发明所述的无标识全动态认证法，用户终端将用户的原始认证标识码和认
证码进行动态加密后传送至服务器，服务器对动态的认证标识码和认证码解密后
进行用户身份确认。

本发明采用的认证方法，由于对认证标识码和认证码均进行一动态加密，故
用户每次进行身份认证时，由于每次加密所得的结果均不相同，没有一个静态标
25 识和特征可供辨识，使攻击者无法对用户的认证信息进行跟踪、记录、分析。实
际上造成攻击者破解某一用户的变化规律变成了破解所有用户的变化规律，具有
更高的安全性。

附图说明

图 1 本发明所述的认证方法流程示意图。

30 实施例

如图 1 所示，原始码由认证标识码 I_1, I_2, \dots, I_k ，和认证码 P_1, P_2, \dots, P_k 构成，
认证时，用户终端对上述原始标识码和认证码进行动态加密，得到每次认证都
会发生变化的全动态认证码 $M_1, M_2, \dots, M_k, M_{k+1}, M_{k+2}, \dots, M_{k+n}$ ，然后将此动态
5 标识码 $M_1, M_2, \dots, M_k, M_{k+1}, M_{k+2}, \dots, M_{k+n}$ 传送至服务器上，服务器对上述动态
标识码进行解密得到原始认证标识码 I_1, I_2, \dots, I_k ，和认证码 P_1, P_2, \dots, P_k 后进行
相应的验证。

上述加密过程可由设定在用户终端的加密软件或硬件进行，其对加密方法不
作限定，可采用各种加密技术。例如可通过每次认证采用不同的加密方法来获得
10 动态加密结果；也可以不改变每次认证的加密方法，而由使用不同的密钥来得到
不相同的加密结果，更可以采用动态加密的方法进行。服务器对无标识全动态认
证码的解密可采用与用户终端相同的加密算法体系进行解密；也可以是用户终端
采用私钥加密，服务器采用相应的公钥进行解密。

本发明并不限于上述实施方式，其核心是把标识码和认证码均进行一动态转
换后，不再存在静态的标识码或认证码后传送服务器进行身份认证，故对于那些
15 无认证码，而仅仅保留动态的标识码进行认证的方式也是本发明要求保护的范
围。

权 利 要 求

- 1、一种无标识全动态认证法，其特征在于：用户终端将用户的原始认证标识码和认证码进行动态加密后，得到一无标识全动态认证码传送至服务器，服务器对接收到的无标识全动态认证码解密后进行用户身份确认。
- 5 2、按权利要求 1 所述的无标识全动态认证法，其特征在于：用户终端和服务器采用相同动态加密算法体系进行加密和解密。

1/1

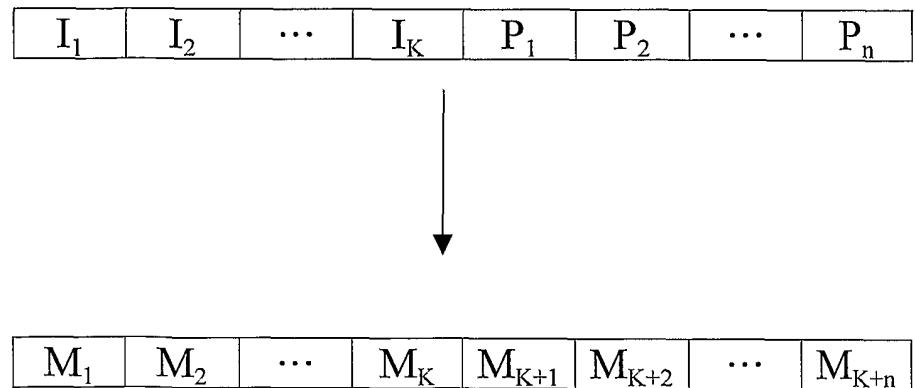


图 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN01/01401

A. CLASSIFICATION OF SUBJECT MATTER

IPC⁷ H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC⁷ H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

WPI ; EPODOC ; CNPAT ; JAP ; UNPATENT JOURNAL OF QINGHUA
encrypt; decrypt; server; Terminal; client; identification; dynamic; identification; authentication

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|-----------|---|-----------------------|
| X | US4720860 Security Dynamics Technologies, Inc., Cambridge, Mass, (19 January 1988) col.1, line 6—col.3, line 45 | 1-2 |
| X | JOURNAL OF XI'AN JIAOTONG UNIVERSITY, Vol.33, No.7, Jul.1999 Li Wei: Net Security Based on Router Dynamic Authentication | 1 |
| A | US4578530 VISA U.S.A., INC., San Mateo, Calif. (25 March 1986) the whole document | 1-2 |

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:

- “A” document defining the general state of the art which is not considered to be of particular relevance
- “E” earlier application or patent but published on or after the international filing date
- “L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)
- “O” document referring to an oral disclosure, use, exhibition or other means
- “P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
10 December 2001 (10.12.01)

Date of mailing of the international search report
27. DEC. 2001 (27.12.01)

Name and mailing address of the ISA/CN
6 Xitucheng Rd., Jimen Bridge, Haidian District,
100088 Beijing, China
Facsimile No. 86-10-62019451

Authorized officer 3316

Telephone No. 86-10-62093856

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN01/01401

| Patent document cited in search report | Publication data | Patent family member(s) | Publication data |
|---|------------------|-------------------------|------------------|
| US4720860 | 19 January 1988 | CA1270957 | 26 June 1990 |

国际检索报告

国际申请号

PCT/CN01/01401

A. 主题的分类IPC⁷ H04L 9/00

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类体系和分类号)

IPC⁷ H04L 9/00

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称和, 如果实际可行的, 使用的检索词)

WPI ; EPODOC ; CNPAT ; 清华非专利期刊; 加密; 解密; 标识码; 服务器; 终端; 动态; 认证; encrypt; decrypt; server; Terminal; client; identification; dynamic; identification; authentication

C. 相关文件

| 类 型* | 引用文件, 必要时, 指明相关段落 | 相关的权利要求编号 |
|------|---|-----------|
| X | US4720860 Security Dynamics Technologies, Inc., Cambridge, Mass, (19.1 月 1988 年) 说明书第 1 栏第 6 行至第 3 栏第 45 行 | 1-2 |
| X | 西安交通大学学报, 第 33 卷第 7 期, 1999 年 7 月 李卫: 基于路由器动态认证的网络安全 | 1 |
| A | US4578530 VISA U.S.A., INC., San Mateo, Calif. (25. 3 月 1986 年) 全文 | 1-2 |

 其余文件在 C 栏的续页中列出。 见同族专利附件。

* 引用文件的专用类型:

“A” 明确叙述了被认为不是特别相关的一般现有技术的文件

“E” 在国际申请日的当天或之后公布的在先的申请或专利

“L” 可能引起对优先权要求的怀疑的文件, 为确定另一篇
引用文件的公布日而引用的或者因其他特殊理由而引
用的文件

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布的在后文件, 它与申请不相
抵触, 但是引用它是为了理解构成发明基础的理论或原理“X” 特别相关的文件, 仅仅考虑该文件, 权利要求所记载的
发明就不能认为是新颖的或不能认为是有创造性“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件
结合并且这种结合对于本领域技术人员为显而易见时,
权利要求记载的发明不具有创造性

“&” 同族专利成员的文件

| | |
|--|---|
| 国际检索实际完成的日期 10.12 月 2001 (10.12.01) | 国际检索报告邮寄日期 27.12月2001(27.12.01) |
| 国际检索单位名称和邮寄地址 ISA/CN 中国北京市海淀区西土城路 6 号(100088) 传真号: 86-10-62019451 | 受权官员 3316  电话号码: 86-10-62093856 |

国际检索报告
关于同族专利成员的情报

国际申请号
PCT/CN01/01401

| 检索报告中引用的 专利文件 | 公布日期 | 同族专利成员 | 公布日期 |
|------------------|--------------|-----------|--------------|
| US4720860 | 19. 1 月 1988 | CA1270957 | 26. 6 月 1990 |