(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106303755 A
(43)申请公布日 2017.01.04

(21)申请号 201610856659.6

(22)申请日 2016.09.27

(71)申请人 天脉聚源(北京)传媒科技有限公司
地址 100007 北京市东城区安定门东大街28号雍和大厦E座808室

(72)发明人 张新亮

(74)专利代理机构 北京尚伦律师事务所 11477
代理人 张亮

(51)Int.Cl.
H04N 21/835(2011.01)
H04N 21/6377(2011.01)
H04N 21/472(2011.01)
H04N 21/6587(2011.01)
H04L 29/06(2006.01)

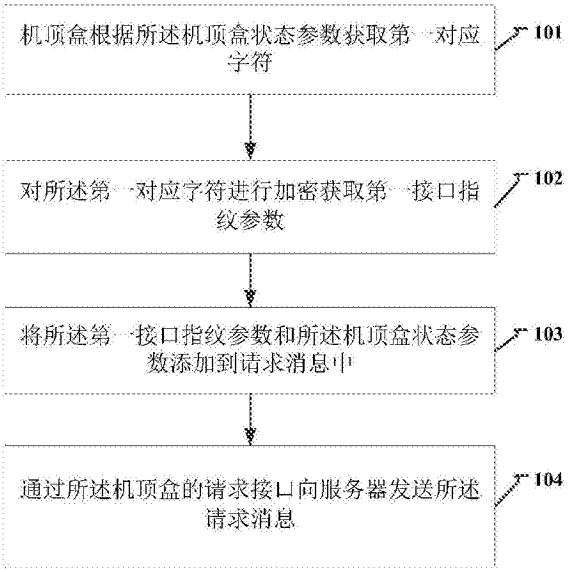
权利要求书1页 说明书8页 附图3页

(54)发明名称

一种接口加密方法、装置和机顶盒登录系统

(57)摘要

本发明公开了一种接口加密方法、装置和机顶盒登录系统。涉及前端信息安全技术领域，解决现有技术中机顶盒的用户请求安全性较差的技术问题。其中，该方法包括：机顶盒根据所述机顶盒状态参数获取第一对应字符；对所述第一对应字符进行加密获取第一接口指纹参数；将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中；通过所述机顶盒的请求接口向服务器发送所述请求消息。



CN 106303755 A

1.一种接口加密方法,其特征在于,包括:

机顶盒根据所述机顶盒状态参数获取第一对应字符;

对所述第一对应字符进行加密获取第一接口指纹参数;

将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中;

通过所述机顶盒的请求接口向服务器发送所述请求消息。

2.根据权利要求1所述的方法,其特征在于,所述机顶盒状态参数包括:产品序列号SN码、软件标识参数、软件版本号参数和时间戳参数。

3.根据权利要求2所述的方法,其特征在于,所述机顶盒根据所述机顶盒状态参数获取第一对应字符包括:

根据SN码、软件标识参数和软件版本参数组成许可字符串;

按照时间戳参数的位数从所述许可字符串中截取出比较字符串;

根据所述比较字符串和所述时间戳参数从预设的编码映射表中获取所述第一对应字符串。

4.一种接口加密装置,其特征在于,包括:

获取模块,用于根据所述机顶盒状态参数获取第一对应字符;

加密模块,用于对所述第一对应字符进行加密获取第一接口指纹参数;

添加模块,用于将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中;

请求模块,用于通过所述机顶盒的请求接口向服务器发送所述请求消息。

5.根据权利要求4所述的装置,其特征在于,所述机顶盒状态参数包括:产品序列号SN码、软件标识参数、软件版本号参数和时间戳参数。

6.根据权利要求5所述的装置,其特征在于,所述获取模块包括:

组成单元,用于根据SN码、软件标识参数和软件版本参数组成许可字符串;

截取单元,用于按照时间戳参数的位数从所述许可字符串中截取出比较字符串;

获取单元,用于根据所述比较字符串和所述时间戳参数从预设的编码映射表中获取所述第一对应字符串。

7.一种机顶盒登录系统,其特征在于,包括机顶盒和服务器;其中,

所述机顶盒包括如权利要求4-6中任意一项所述接口加密装置;

所述服务器,用于从所述请求消息中获的所述第一接口指纹参数,并根据所述机顶盒状态参数对所述第一接口指纹参数的合法性进行验证;若通过所述合法性验证,则接受所述第一请求消息。

8.根据权利要求7所述的系统,其特征在于,所述服务器,具体用于根据所述机顶盒状态参数获取第二对应字符,对所述第二对应字符进行加密获取第二接口指纹参数,根据所述第一接口指纹参数和第二接口指纹参数是否一致了来对所述第一接口指纹参数的合法性进行验证。

9.根据权利要求7或8所述的系统,其特征在于,所述服务器,还用于若未通过所述合法性验证,则拒绝所述请求消息,并启动安全防护措施。

10.根据权利要求7或8所述的系统,其特征在于,所述机顶盒状态参数包括:产品序列号SN码、软件标识参数、软件版本号参数和时间戳参数。

一种接口加密方法、装置和机顶盒登录系统

技术领域

[0001] 本发明涉及前端信息安全技术领域，特别涉及一种接口加密方法、装置和机顶盒登录系统。

背景技术

[0002] 机顶盒是一个连接电视机与外部信号源的设备。它可以将压缩的数字信号转成电视内容，并在电视机上显示出来。信号可以来自有线电缆、卫星天线、宽带网络以及地面广播。机顶盒接收的内容除了模拟电视可以提供的图像、声音之外，更在于能够接收数字内容，包括电子节目指南、因特网网页、字幕等等。使用户能在现有电视机上观看数字电视节目，并可通过网络进行交互式数字化娱乐、教育和商业化活动。目前，机顶盒具有很多功能，如电子节目指南(EPG)、高速数据广播、软件在线升级、因特网接入和电子邮件。有条件接收。新一代机顶盒的功能用应还包括：①接收广播方式的模拟电视和数字电视节目，②高速访问Internet，收发e-mail，③视频点播(VOD)和音乐点播功能，④电话、可视电话、会议电视，⑤连接VCR、VCD等消费电子产品的功能，⑥电子购物，⑦电子游戏等。

[0003] 数字电视机顶盒的工作过程通常为：数字电视机顶盒通过网络接口模块选择频道，并进行解调和信道解码处理，输出MPEG-2多节目传输流数据，送给解复用器，解复用器从MPEG-2传输流数据中抽出一个节目的已打包的视音频基本流(PES)数据，包括机顶盒视频PES，音频PES和辅助数据PES，解复用器中包含一个解扰引擎，可在传输流层和PES层对加扰的数据进行解扰，解复用器输出的是已解扰的视音频PES。视频PES送入视频解码器，取出MPEG-2视频数据并对其解码后，输出到模拟编码器，编码成模拟视频信号，再经视频输出电路输出。音频PES送入音频解码器，取出MPEG-2音频数据并对其解码，输出PCM音频数据到音频D/A变换器，音频D/A变换器输出模拟立体声音频信号，经音频输出电路输出。

[0004] 随着机顶盒的功能越来越多，其在用户日常生活起到的作用就越来越重要，因此机顶盒的信息安全也变得越来越重要。如付费功能，观看的节目的选择等等，若用户的登录账号信息，请求接口被盗取，则可能出现非用户本意的请求，因此将会严重影响用户的信息安全。

发明内容

[0005] 本发明提供一种接口加密方法、装置和机顶盒登录系统，用于解决现有技术中机顶盒的用户请求安全性较差的技术问题。

[0006] 本发明实施例提供一种接口加密方法，包括：

[0007] 机顶盒根据所述机顶盒状态参数获取第一对应字符；

[0008] 对所述第一对应字符进行加密获取第一接口指纹参数；

[0009] 将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中；

[0010] 通过所述机顶盒的请求接口向服务器发送所述请求消息。

[0011] 本发明实施例提供的方法中，通过采用机顶盒根据所述机顶盒状态参数获取第一

对应字符；对所述第一对应字符进行加密获取第一接口指纹参数；将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中，并通过所述机顶盒的请求接口向服务器发送所述请求消息的技术手段，实现请求消息中携带加密过的第一接口指纹参数，该第一接口指纹参数是根据机顶盒状态参数获取到的，相当于对请求消息进行加密，解决了现有技术中请求消息被盗取所导致的安全性较差的技术问题，进而实现了即便获取到了机顶盒的请求接口或者登录账户等信息，由于没有正确的第一接口指纹参数，通过不了服务器针对该第一接口指纹参数设置的安全验证机制，进而仍旧无法得到服务器响应的效果，保证用户机顶盒登录请求消息安全性的技术效果。

[0012] 可选的，所述机顶盒状态参数包括：产品序列号SN码、软件标识参数、软件版本号参数和时间戳参数。

[0013] 可选的额，所述机顶盒根据所述机顶盒状态参数获取第一对应字符包括：

[0014] 根据SN码、软件标识参数和软件版本参数组成许可字符串；

[0015] 按照时间戳参数的位数从所述许可字符串中截取出比较字符串；

[0016] 根据所述比较字符串和所述时间戳参数从预设的编码映射表中获取所述第一对应字符串。

[0017] 本发明实施例提供的方法中，第一对应字符是根据机顶盒状态参数获取到的，由于计算方法的不同，机顶盒状态参数的变化性等原因，即便请求接口被盗取，仍旧用该请求接口同样去向服务器请求的消息由于第一对应字符的不同，导致第一接口指纹参数不同，进而携带的第一接口指纹参数通不过验证，因此可以取得通过第一对应字符来保证机顶盒处用户请求安全性的技术效果。

[0018] 基于同样的发明构思，本发明实施例继续提供一种接口加密装置，包括：

[0019] 获取模块，用于根据所述机顶盒状态参数获取第一对应字符；

[0020] 加密模块，用于对所述第一对应字符进行加密获取第一接口指纹参数；

[0021] 添加模块，用于将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中；

[0022] 请求模块，用于通过所述机顶盒的请求接口向服务器发送所述请求消息。

[0023] 本发明实施例提供的装置中，具有根据所述机顶盒状态参数获取第一对应字符；对所述第一对应字符进行加密获取第一接口指纹参数；将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中，并通过所述机顶盒的请求接口向服务器发送所述请求消息的功能，实现请求消息中携带加密过的第一接口指纹参数，该第一接口指纹参数是根据机顶盒状态参数获取到的，相当于对请求消息进行加密，解决了现有技术中请求消息被盗取所导致的安全性较差的技术问题，进而实现了即便获取到了机顶盒的请求接口或者登录账户等信息，由于没有正确的第一接口指纹参数，仍旧无法得到服务器响应，保证用户机顶盒登录请求消息安全性的技术效果。

[0024] 可选的，所述机顶盒状态参数包括：产品序列号SN码、软件标识参数、软件版本号参数和时间戳参数。

[0025] 可选的，所述获取模块包括：

[0026] 组成单元，用于根据SN码、软件标识参数和软件版本参数组成许可字符串；

[0027] 截取单元，用于按照时间戳参数的位数从所述许可字符串中截取出比较字符串；

[0028] 获取单元，用于根据所述比较字符串和所述时间戳参数从预设的编码映射表中获取所述第一对应字符串。

[0029] 基于同样的发明构思，本发明实施例继续提供一种机顶盒登录系统，包括机顶盒和服务器；其中，

[0030] 所述机顶盒包括上述任意一项所述接口加密装置；

[0031] 所述服务器，用于从所述请求消息中获的所述第一接口指纹参数，并根据所述机顶盒状态参数对所述第一接口指纹参数的合法性进行验证；若通过所述合法性验证，则接受所述第一请求消息。

[0032] 本发明实施例提供的系统中，机顶盒将根据机顶盒状态参数得出的经过加密的第一接口指纹参数添加到请求消息中的手段，为该请求消息进行了加密，服务器通过对该加密的第一接口指纹参数进行合法性验证，并在通过该验证后再接受该请求消息的请求内容的方案来实现保证用户请求消息的安全性的技术效果。

[0033] 可选的，所述服务器，具体用于根据所述机顶盒状态参数获取第二对应字符，对所述第二对应字符进行加密获取第二接口指纹参数，根据所述第一接口指纹参数和第二接口指纹参数是否一致了来对所述第一接口指纹参数的合法性进行验证。

[0034] 本发明实施例提供的系统中，在接收到包含有第一接口指纹参数的请求消息后，采用同样的方法，根据机顶盒状态参数来计算出第二接口指纹参数，根据第一和第二接口指纹参数是否一致来确定该请求消息是否合法，进而取得保证用户请求消息是真正来自用户的请求，保证用户请求安全性的技术效果。

[0035] 可选的，所述服务器，还用于若未通过所述合法性验证，则拒绝所述请求消息，并启动安全防护措施。

[0036] 可选的，所述机顶盒状态参数包括：产品序列号SN码、软件标识参数、软件版本号参数和时间戳参数。

[0037] 本发明实施例提供的系统中，针对未通过合法性验证的请求消息可以直接拒绝该请求，并启动安全防护措施，有效的保护机顶盒请求消息的安全。

[0038] 本发明的其它特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

[0039] 下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

附图说明

[0040] 附图用来提供对本发明的进一步理解，并且构成说明书的一部分，与本发明的实施例一起用于解释本发明，并不构成对本发明的限制。在附图中：

[0041] 图1为本发明实施例一中提供的一种接口加密方法的流程图；

[0042] 图2为本发明实施例二中提供的一种接口加密方法的流程图；

[0043] 图3为本发明实施例二中提供的一种接口加密装置的结构示意图；

[0044] 图4为本发明实施例三中提供的一种机顶盒登录系统的结构示意图。

具体实施方式

[0045] 以下结合附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。

[0046] 实施例一

[0047] 本发明实施例提供一种接口加密方法，该方法适合部署在机顶盒上，如图1所示，该方法包括：

[0048] 101，机顶盒根据所述机顶盒状态参数获取第一对应字符；

[0049] 可选的，所述机顶盒状态参数包括：产品序列号SN码、软件标识参数、软件版本号参数和时间戳参数。

[0050] 可选的，上述101可通过如下方式实现：

[0051] 根据SN码、软件标识参数和软件版本参数组成许可字符串；

[0052] 按照时间戳参数的位数从所述许可字符串中截取出比较字符串；

[0053] 根据所述比较字符串和所述时间戳参数从预设的编码映射表中获取所述第一对应字符串。

[0054] 本发明实施例提供的方法中，第一对应字符是根据机顶盒状态参数获取到的，由于计算方法的不同，机顶盒状态参数的变化性等原因，即便请求接口被盗取，仍旧用该请求接口同样去向服务器请求的消息由于第一对应字符的不同，导致第一接口指纹参数不同，进而携带的第一接口指纹参数通不过验证，因此可以取得通过第一对应字符来保证机顶盒处用户请求安全性的技术效果。

[0055] 102，对所述第一对应字符进行加密获取第一接口指纹参数；

[0056] 可采用base64加密方法对所述第一对应字符进行加密得到加密串第一接口指数参数。

[0057] 其中，第一对应字符与所述机顶盒状态参数的对应关系包括：对应的和与对应关系相反的关系。

[0058] 103，将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中；

[0059] 104，通过所述机顶盒的请求接口向服务器发送所述请求消息，以保证所述请求消息的安全性。

[0060] 本发明实施例提供的方法中，通过采用机顶盒根据所述机顶盒状态参数获取第一对应字符；对所述第一对应字符进行加密获取第一接口指纹参数；将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中，并通过所述机顶盒的请求接口向服务器发送所述请求消息的技术手段，实现请求消息中携带加密过的第一接口指纹参数，该第一接口指纹参数是根据机顶盒状态参数获取到的，相当于对请求消息进行加密，解决了现有技术中请求消息被盗取所导致的安全性较差的技术问题，进而实现了即便获取到了机顶盒的请求接口或者登录账户等信息，由于没有正确的第一接口指纹参数，通过不了服务器针对该第一接口指纹参数设置的安全验证机制，进而仍旧无法得到服务器响应的效果，保证用户机顶盒登录请求消息安全性的技术效果。

[0061] 实施例二

[0062] 本发明实施例具体以机顶盒发送登录请求消息到BOSS服务器为例，提供一种接口加密方法，如图2所示，该方法包括：

[0063] 本实施例中提供的方法中，该接口加密方式为接口中一个参数，即第一接口指纹

参数为根据另外4个参数加密算出来的，因此即使别人通过破解方式获取到了机顶盒的请求接口，用这个相同的接口去请求也是不能用的，具体加密方式如下：

[0064] 在机顶盒登陆接口中finger_print(第一接口指纹)参数为机顶盒的SN码参数(stb_no)，软件标识参数(software_code)，软件版本号参数(software_version)，时间戳参数(tk)这四个参数动态加密算出来的，算法如下：

[0065] 201，机顶盒根据所述机顶盒状态参数中的SN码、软件标识参数和软件版本参数组成许可字符串；

[0066] 例如：.将SN码(sn)，软件标识(softwareCode)，软件编码(softwareVersion)这三个字符串组成一个字符串。

[0067] 其中，SN码数字+字母组成如：abc12443；其中，软件编码数字.数字.数字三个号段组成如：0.1.23；

[0068] 可选的，所述机顶盒状态参数包括：产品序列号SN码、软件标识参数、软件版本号参数和时间戳参数。

[0069] 可选的，在该步骤200过程中或者之前，还可以预设编码映射表：

[0070] 例如预设的编码表为：

[0071] #编码映射

[0072] CODE_MAP＝{["a"]＝0,["b"]＝1,["c"]＝2,["d"]＝3,["e"]＝4,["f"]＝5,["g"]＝6,["h"]＝7,["i"]＝8,["j"]＝9,["k"]＝10,["l"]＝11,["m"]＝12,["n"]＝13,["o"]＝14,["p"]＝15,["q"]＝16,["r"]＝17,["s"]＝18,["t"]＝19,["u"]＝20,["v"]＝21,["w"]＝22,["x"]＝23,["y"]＝24,["z"]＝25,

[0073] ["A"]＝26,["B"]＝27,["C"]＝28,["D"]＝29,["E"]＝30,["F"]＝31,["G"]＝32,["H"]＝33,["I"]＝34,["J"]＝35,["K"]＝36,["L"]＝37,["M"]＝38,["N"]＝39,["O"]＝40,["P"]＝41,["Q"]＝42,["R"]＝43,["S"]＝44,["T"]＝45,["U"]＝46,["V"]＝47,["W"]＝48,["X"]＝49,["Y"]＝50,["Z"]＝51,

[0074] ["1"]＝52,["2"]＝53,["3"]＝54,["4"]＝55,["5"]＝56,["6"]＝57,["7"]＝58,["8"]＝59,["9"]＝60,["0"]＝61,["-"]＝62,["_"]＝63,["@"]＝64,["."]＝65

[0075] 202，按照时间戳参数的位数从所述许可字符串中截取出比较字符串；

[0076] 例如时间戳参数是13位，则将这个许可字符串截取前13位得出比较字符串：

[0077] 203，根据所述比较字符串和所述时间戳参数从预设的编码映射表中获取所述第一对应字符串。

[0078] 可选的，该202可具体通过如下方式实现：

[0079] 取出13位比较可符串的每一位，并去编码映射表找出第一对应值；以及取出13位时间戳参数中的每一位数字，并去编码映射表找出第二对应值；将分别找出的第一和第二对应值的两个值相加，若大于编码映射表的长度，则用这个数减去编码映射表的长度得出一个新的值；根据这个值去编码映射表中找不对应的字符(也可以是对应的字符，但不管是否为对应的字符，都可以是本实施例中的第一对应字符)。

[0080] 204，对所述第一对应字符进行加密获取第一接口指纹参数；

[0081] 可采用base64加密方法对所述第一对应字符进行加密得到加密串第一接口指数参数。

[0082] 205，将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中；

[0083] 206，通过所述机顶盒的请求接口向BOSS服务器发送所述请求消息，以保证所述请求消息的安全性。

[0084] 207，BOSS服务器接到请求消息后，会用同201-204的方法来验证这个第一接口指纹参数是否合法；若不是这个方法得出来的，则有可能是恶意请求，执行208；否则，认为该请求合法，执行209；

[0085] 208，BOSS服务器直接拒绝请求，启动安全防护措施。

[0086] 该安全防护措施如报警，加入黑名单，提示工作人员或用户等。

[0087] 209，响应该请求消息所述请求的内容。

[0088] 本发明实施例提供的方法中，通过采用机顶盒根据所述机顶盒状态参数获取第一对应字符；对所述第一对应字符进行加密获取第一接口指纹参数；将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中，并通过所述机顶盒的请求接口向服务器发送所述请求消息的技术手段，实现请求消息中携带加密过的第一接口指纹参数，该第一接口指纹参数是根据机顶盒状态参数获取到的，相当于对请求消息进行加密，解决了现有技术中请求消息被盗取所导致的安全性较差的技术问题，进而实现了即便获取到了机顶盒的请求接口或者登录账户等信息，由于没有正确的第一接口指纹参数，通过不了服务器针对该第一接口指纹参数设置的安全验证机制，进而仍旧无法得到服务器响应的效果，保证用户机顶盒登录请求消息安全性的技术效果。

[0089] 实施例三

[0090] 为了便于上述实施例一、二中机顶盒侧的方法实现，本发明实施例继续提供一种接口加密装置，该接口加密装置可以安装在机顶盒中。如图3所示，包括：

[0091] 获取模块31，用于根据所述机顶盒状态参数获取第一对应字符；

[0092] 加密模块32，用于对所述第一对应字符进行加密获取第一接口指纹参数；

[0093] 添加模块33，用于将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中；

[0094] 请求模块34，用于通过所述机顶盒的请求接口向服务器发送所述请求消息。

[0095] 可选的，所述机顶盒状态参数包括：产品序列号SN码、软件标识参数、软件版本号参数和时间戳参数。

[0096] 可选的，所述获取模块31包括：

[0097] 组成单元，用于根据SN码、软件标识参数和软件版本参数组成许可字符串；

[0098] 截取单元，用于按照时间戳参数的位数从所述许可字符串中截取出比较字符串；

[0099] 获取单元，用于根据所述比较字符串和所述时间戳参数从预设的编码映射表中获取所述第一对应字符串。

[0100] 本发明实施例提供的装置中，具有根据所述机顶盒状态参数获取第一对应字符；对所述第一对应字符进行加密获取第一接口指纹参数；将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中，并通过所述机顶盒的请求接口向服务器发送所述请求消息的功能，实现请求消息中携带加密过的第一接口指纹参数，该第一接口指纹参数是根据机顶盒状态参数获取到的，相当于对请求消息进行加密，解决了现有技术中请求消息被盗取所导致的安全性较差的技术问题，进而实现了即便获取到了机顶盒的请求接口或者登录

账户等信息，由于没有正确的第一接口指纹参数，仍旧无法得到服务器响应，保证用户机顶盒登录请求消息安全性的技术效果。

[0101] 实施例四

[0102] 本发明实施例继续提供一种机顶盒登录系统，如图4所示，包括机顶盒41和服务器42；该服务器42可以具体为BOSS服务器。其中，

[0103] 所述机顶盒41包括上述实施例三种所述接口加密装置；

[0104] 所述服务器42，用于从所述请求消息中获的所述第一接口指纹参数，并根据所述机顶盒状态参数对所述第一接口指纹参数的合法性进行验证；若通过所述合法性验证，则接受所述第一请求消息。

[0105] 本发明实施例提供的系统中，机顶盒将根据机顶盒状态参数得出的经过加密的第一接口指纹参数添加到请求消息中的手段，为该请求消息进行了加密，服务器通过对该加密的第一接口指纹参数进行合法性验证，并在通过该验证后再接受该请求消息的请求内容的方案来实现保证用户请求消息的安全性的技术效果。

[0106] 可选的，所述服务器42，具体用于根据所述机顶盒状态参数获取第二对应字符，对所述第二对应字符进行加密获取第二接口指纹参数，根据所述第一接口指纹参数和第二接口指纹参数是否一致了来对所述第一接口指纹参数的合法性进行验证。

[0107] 本发明实施例提供的系统中，在接收到包含有第一接口指纹参数的请求消息后，采用同样的方法，根据机顶盒状态参数来计算出第二接口指纹参数，根据第一和第二接口指纹参数是否一致来确定该请求消息是否合法，进而取得保证用户请求消息是真正来自用户的请求，保证用户请求安全性的技术效果。

[0108] 可选的，所述服务器42，还用于若未通过所述合法性验证，则拒绝所述请求消息，并启动安全防护措施。

[0109] 可选的，所述机顶盒状态参数包括：产品序列号SN码、软件标识参数、软件版本号参数和时间戳参数。

[0110] 本发明实施例提供的系统中，针对未通过合法性验证的请求消息可以直接拒绝该请求，并启动安全防护措施，有效的保护机顶盒请求消息的安全。

[0111] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器和光学存储器等)上实施的计算机程序产品的形式。

[0112] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0113] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指

令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0114] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0115] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

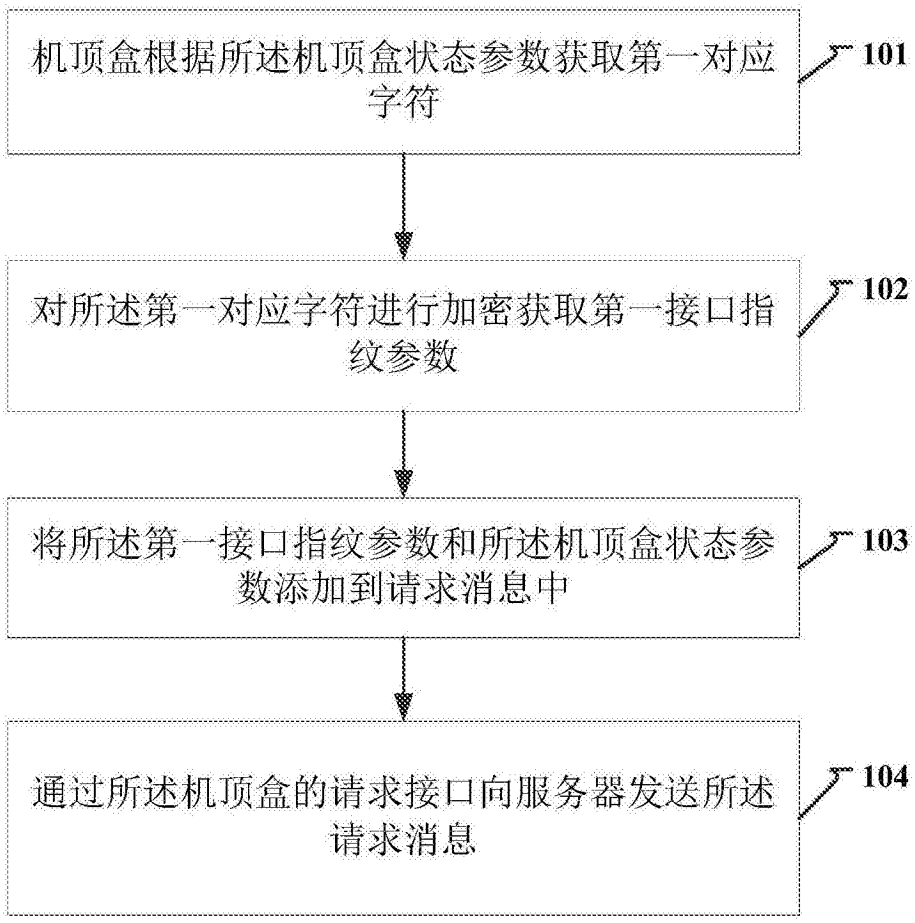

机顶盒根据所述机顶盒状态参数获取第一对应字符
101
对所述第一对应字符进行加密获取第一接口指纹参数
102
将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中
103
通过所述机顶盒的请求接口向服务器发送所述请求消息
104

图1

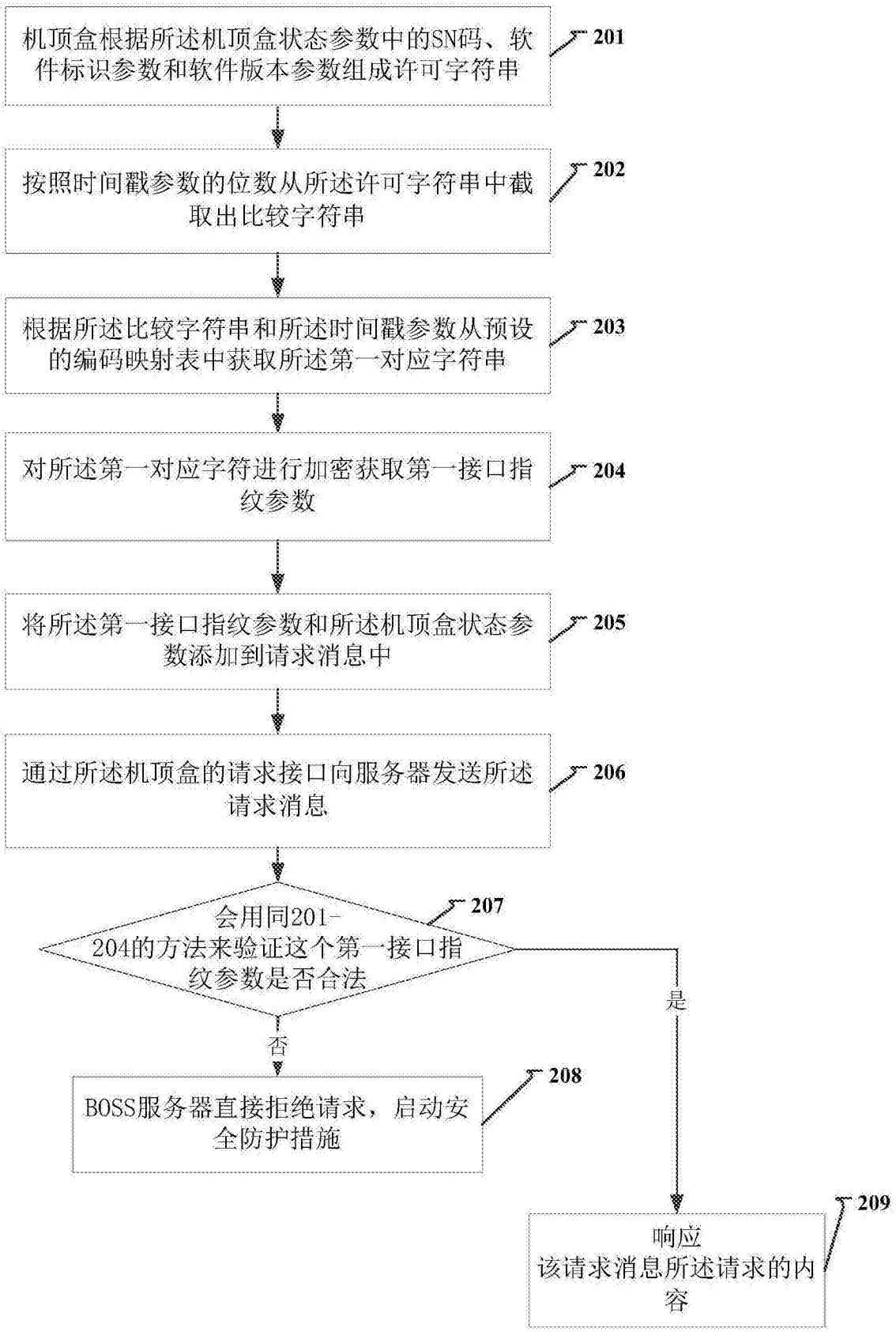

机顶盒根据所述机顶盒状态参数中的SN码、软件标识参数和软件版本参数组成许可字符串
201
按照时间戳参数的位数从所述许可字符串中截取出比较字符串
202
根据所述比较字符串和所述时间戳参数从预设的编码映射表中获取所述第一对应字符串
203
对所述第一对应字符进行加密获取第一接口指纹参数
204
将所述第一接口指纹参数和所述机顶盒状态参数添加到请求消息中
205
通过所述机顶盒的请求接口向服务器发送所述请求消息
206
会用同201-204的方法来验证这个第一接口指纹参数是否合法
207
是
否
BOSS服务器直接拒绝请求，启动安全防护措施
208
响应该请求消息所述请求的内容
209

图2

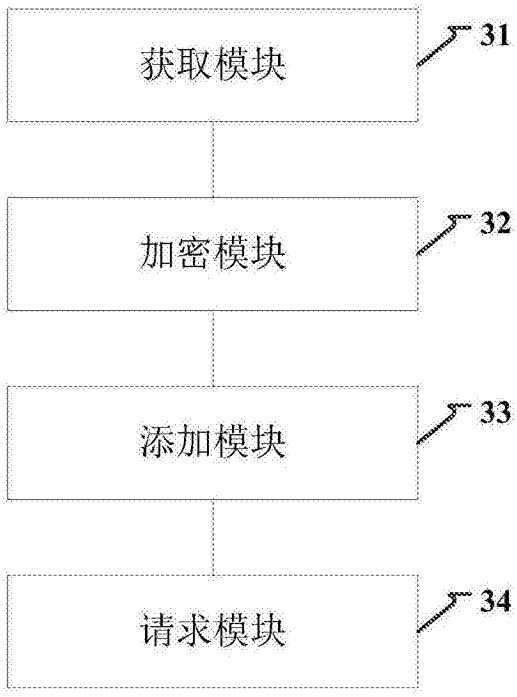


图3

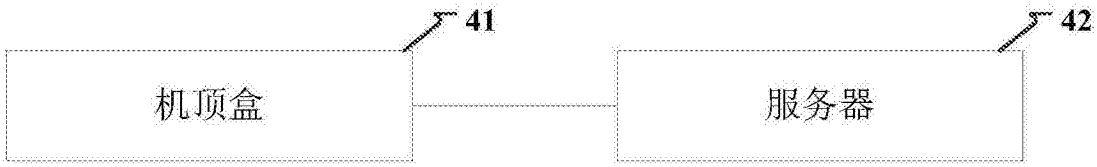


图4