[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 5/00 (2006.01)
G06F 9/445 (2006.01)

[12] 发明专利说明书

专利号 ZL 200710119226.3

[45] 授权公告日 2009 年 12 月 23 日

[11] 授权公告号 CN 100574367C

[22] 申请日 2007.7.18
[21] 申请号 200710119226.3
[73] 专利权人 中国联合网络通信集团有限公司
地址 100140 北京市西城区金融大街 21 号
[72] 发明人 王 彬
[56] 参考文献
CN1764268A 2006.4.26
WO2005003936A1 2005.1.13
CN1960363A 2007.5.9
US2004187011A1 2003.9.23
CN1422404A 2003.6.4
审查员 苏玉磊

[74] 专利代理机构 北京同立钧成知识产权代理有限公司
代理人 刘 芳

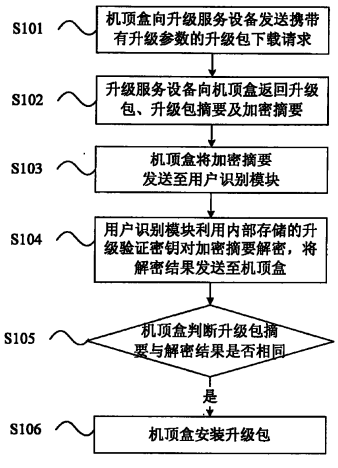
权利要求书 2 页 说明书 6 页 附图 3 页

[54] 发明名称

机顶盒软件升级方法及升级系统

[57] 摘要

本发明涉及机顶盒软件升级方法及升级系统，机顶盒向升级服务设备发送升级包下载请求，升级包下载请求中携带有机顶盒的升级参数；升级服务设备根据升级参数将升级包、升级包摘要及对升级包摘要加密得到的加密摘要下载至机顶盒；机顶盒将加密摘要发送至用户识别模块；用户识别模块根据内部存储的升级验证密钥对加密摘要解密得到解密结果；机顶盒在升级包摘要与解密结果相同时，安装升级包。 本发明通过对升级包的验证增强了机顶盒软件升级的安全性，降低了机顶盒被恶意攻击的可能性；将升级验证密存储于用户识别模块中并由用户识别模块完成解密运算，密钥不会泄露到用户识别模块之外，从而进一步增强了安全性。



1、 一种机顶盒软件更新方法，其特征在于，所述方法包括如下步骤：

机顶盒向升级服务设备发送升级包下载请求，所述升级包下载请求中携带有所述机顶盒的升级参数；

所述升级服务设备根据所述升级参数将升级包、升级包摘要及对所述升级包摘要加密得到的加密摘要下载至所述机顶盒；

所述机顶盒将所述加密摘要发送至用户识别模块；

所述用户识别模块根据内部存储的升级验证密钥对所述加密摘要解密得到解密结果；

所述机顶盒在所述升级包摘要与所述解密结果相同时，安装所述升级包。

2、 根据权利要求 1 所述的机顶盒软件更新方法，其特征在于，所述升级服务设备根据所述升级参数将升级包、升级包摘要及对所述升级包摘要加密得到的加密摘要下载至所述机顶盒具体为：所述升级服务设备根据所述升级参数在本地进行检索，将检索到的升级包、升级包摘要以及对所述升级包摘要加密得到的加密摘要下载至机顶盒。

3、 根据权利要求 1 所述的机顶盒软件更新方法，其特征在于，所述升级服务设备根据所述升级参数将升级包、升级包摘要及对所述升级包摘要加密得到的加密摘要下载至所述机顶盒具体为：所述升级服务设备根据所述升级参数在本地检索升级包，生成升级包摘要，并对升级包摘要加密生成加密摘要，然后将升级包、升级包摘要以及对所述升级包摘要加密得到的加密摘要下载至机顶盒。

4、 根据权利要求 3 所述的机顶盒软件更新方法，其特征在于，所述升级包下载请求中携带有用户标识信息，对升级包摘要加密之前，所述升级服务设备根据所述用户标识信息查找对应的加密密钥。

5、 根据权利要求 1-4 任一所述的机顶盒软件更新方法，其特征在于，所述方法还包括：所述机顶盒将升级包摘要发送至所述用户识别模块；在得

到解密结果后，所述用户识别模块判断所述升级包摘要与所述解密结果是否相同，并将判断结果发送至机顶盒。

6、 根据权利要求 1-4 任一所述的机顶盒软件更新方法，其特征在于，在得到解密结果后，所述用户识别模块将解密结果发送至所述机顶盒；所述机顶盒判断所述升级包摘要与所述解密结果是否相同。

7、 一种机顶盒软件升级系统，其特征在于，所述系统包括:

机顶盒，用于向升级服务设备发送携带有升级参数的升级包下载请求，接收所述升级服务设备返回的升级包、升级包摘要以及加密摘要，并将所述加密摘要发送至用户识别模块解密，在所述升级包摘要与解密结果相同时，安装所述升级包;

升级服务设备，用于根据所述升级包下载请求携带的升级参数，将升级包、升级包摘要以及对所述升级包摘要加密得到的加密摘要下载至所述机顶盒;

用户识别模块，用于存储升级验证密钥，并利用所述升级验证密钥对所述加密摘要解密得到解密结果。

机顶盒软件升级方法及升级系统

技术领域

本发明涉及通信技术，尤其涉及机顶盒软件升级方法、升级系统、机顶盒、用户识别模块以及升级服务设备。

背景技术

网络电视（Internet Protocol Television，简称 IPTV）业务是一个全新的业务模式，它给消费者带来的是集信息、娱乐、学习、购物于一体的网络享受。现有电视可以通过 IPTV 机顶盒（Set Top Box，简称 STB）使用 IPTV 业务。

在机顶盒的实际使用过程中，由于相关新业务的不断推出，机顶盒需要不定期地针对新业务安装业务插件，并且，机顶盒本身软件平台也需要不断修补漏洞，这都需要对机顶盒进行软件升级。

现有的一种机顶盒软件升级方法是由机顶盒自主下载插件，机顶盒并不对插件进行合法性认证。但是，在现阶段，网络中为窃取用户信息而编制的恶意软件包比比皆是，这种机顶盒软件升级方法存在严重的安全隐患，升级包的合法性验证是需要解决的一个关键问题。

现有的另一种机顶盒软件升级方法是由机顶盒在其内部完成升级包的认证。在出厂时，密钥固化于机顶盒内部，软件升级时，机顶盒根据该密钥对升级包进行认证。这种方法需要机顶盒提供完善的安全机制，但是，现有机顶盒的安全机制并不能满足软件升级的安全需求。

发明内容

本发明所要解决的技术问题是，提供机顶盒软件升级方法，增强机顶盒软件升级的安全性，降低机顶盒被恶意攻击的可能性。

为了解决上述技术问题，本发明提供了一种机顶盒软件更新方法，所述方法包括如下步骤：机顶盒向升级服务设备发送升级包下载请求，所述升级包下载请求中携带有所述机顶盒的升级参数；所述升级服务设备根据所述升级参数将升级包、升级包摘要及对所述升级包摘要加密得到的加密摘要下载至所述机顶盒；所述机顶盒将所述加密摘要发送至用户识别模块；所述用户识别模块根据内部存储的升级验证密钥对所述加密摘要解密得到解密结果；所述机顶盒在所述升级包摘要与所述解密结果相同时，安装所述升级包。

为了解决上述技术问题，本发明还提供了一种机顶盒软件升级方法，所述方法包括如下步骤：向升级服务设备发送携带有升级参数的升级包下载请求；接收所述升级服务设备返回的升级包，升级包摘要及对所述升级包的摘要加密后得到的加密摘要；将所述加密摘要发送至用户识别模块进行解密；

在所述升级包摘要与解密结果相同时，安装所述升级包。

为了解决上述技术问题，本发明再提供了一种机顶盒软件升级系统，所述系统包括：机顶盒，用于向升级服务设备发送携带有升级参数的升级包下载请求，接收所述升级服务设备返回的升级包、升级包摘要以及加密摘要，并将所述加密摘要发送至用户识别模块解密，在所述升级包摘要与解密结果相同时，安装所述升级包；升级服务设备，用于根据所述升级包下载请求携带的升级参数，将升级包、升级包摘要以及对所述升级包摘要加密得到的加密摘要下载至所述机顶盒；用户识别模块，用于存储升级验证密钥，并利用所述升级验证密钥对所述加密摘要解密得到解密结果。

本发明通过对升级包的验证增强了机顶盒软件升级的安全性，降低了机顶盒被恶意攻击的可能性；将升级验证密存储于用户识别模块中，并由用户识别模块完成解密运算，密钥不会泄露到用户识别模块之外，从而进一步增强了安全性。

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

图 1 为应用本发明的机顶盒软件升级方法的系统结构示意图;

图 2 为本发明的机顶盒软件升级方法实施例一流程图;

图 3 为本发明的机顶盒软件升级方法实施例二流程图。

具体实施方式

如图 1 所示，为应用本发明的机顶盒软件升级方法的系统结构示意图。该系统包括: 机顶盒 10, 用户识别模块(Subscriber Identity Module, 简称 SIM) 20 以及升级服务设备 30。

机顶盒 10 为待进行软件升级的设备，在需要进行软件升级时，机顶盒 10 向升级服务器 30 发送携带有升级参数的升级包下载请求，升级参数可以包括机顶盒的硬件版本号、操作系统版本号等参数。

升级服务器 30 中存储有各种机顶盒的升级包，根据升级参数将对应的升级包、升级包摘要及对升级包摘要加密得到的加密摘要下载至机顶盒 10。其中，升级包摘要及加密摘要用于升级包的合法性验证，升级包摘要及加密摘要可以事先生成，并存储于升级服务设备 30 中，在下载时，直接根据升级参数检索对应的升级包、升级包摘要及加密摘要即可。升级包摘要及加密摘要也可实时生成，这样，安全性会更好一些，升级服务设备根据升级参数检索升级包，生成升级包摘要，并对升级包摘要加密生成加密摘要。下载可采用 FTP 方式，HTTP 方式等。对升级包摘要的加解密可采用现有的任一种加解密方法，如 3DES 算法、 MD5 算法等。

用户识别模块 20 存储有升级包验证密钥，并能利用该密钥进行解密运算。机顶盒 10 接收到升级服务设备 30 返回的升级包、升级包摘要及加密摘要后，将加密摘要发送至用户识别模块 20，由用户识别模块 20 利用内部存储的升级验证密钥对加密摘要进行解密。当解密结果与升级包摘要相同时，验证通过，机顶盒 10 安装升级包。解密结果与升级包摘要是否相同可以由机

顶盒 10 判断，也可由用户识别模块 20 判断。在由用户识别模块 20 判断时，机顶盒需将升级包摘要发送至用户识别模块 20。

如图 2 所示，为本发明的机顶盒软件升级方法实施例一流程图。本实施例包括如下步骤:

步骤 S101、机顶盒向升级服务设备发送携带有升级参数的升级包下载请求;

步骤 S102、升级服务设备根据升级包下载请求携带的升级参数，在本地检索升级包，生成升级包摘要，并对升级包摘要加密生成加密摘要，将升级包、升级包摘要以及加密摘要下载至机顶盒;

升级报摘要及加密摘要为验证数据；可根据实际情况确定升级包摘要及加密摘要的长度，例如，采用 32 字节的验证数据，其中，前 16 字节为升级包摘要，后 16 字节为加密摘要;

步骤 S103、机顶盒接收升级包、升级包摘要以及加密摘要，并将加密摘要发送至用户识别模块;

步骤 S104、用户识别模块利用内部存储的升级验证密钥对加密摘要解密得到解密结果，并将解密结果发送至机顶盒;

步骤 S105、机顶盒判断升级包摘要与解密结果是否相同，若相同，验证通过，执行步骤 S106；若不同，验证未通过，不安装升级包;

步骤 S106、机顶盒安装下载的升级包。

本实施例通过对升级包摘要加解密实现了升级包的合法性验证，可有效防止恶意软件对终端的攻击；升级验证密钥的存储和加密摘要的解密由用户识别模块完成，充分利用用户识别模块存储保密性高、解密算法内置的特点，密钥不会泄露到用户识别模块之外，可有效增强安全性。

如图 3 所示，为本发明的机顶盒软件升级方法实施例二流程图。本实施例中，不同的用户拥有不同的升级验证密钥，升级服务设备中存储有用户标识与加密密钥的对应关系。接收到升级包下载请求后，升级服务设备根据请

求中携带的用户标识查找相应的加密密钥，利用该加密密钥对升级包摘要加密。本实施例包括如下步骤:

步骤 S201、机顶盒向升级服务设备发送携带有升级参数及用户标识的升级包下载请求；其中，用户标识可以为用户识别模块的标识;

步骤 S202、升级服务设备根据升级参数在本地检索升级包，生成升级包摘要;

步骤 S203、升级服务设备根据用户标识检索对应的加密密钥;

步骤 S204、升级服务设备利用检索到的加密密钥对升级包摘要加密;

步骤 S205、升级服务器将升级包、升级包摘要以及加密摘要下载至机顶盒;

步骤 S206、机顶盒接收升级包、升级包摘要以及加密摘要，并将升级包摘要及加密摘要发送至用户识别模块;

步骤 S207、用户识别模块利用内部存储的升级验证密钥对加密摘要解密得到解密结果;

步骤 S208、用户识别模块判断升级包摘要与解密结果是否相同，并将判断结果发送至机顶盒;

步骤 S209、机顶盒根据判断结果判断验证是否通过，若升级包摘要与解密结果相同，验证通过，执行步骤 S210；若不同，验证未通过，不安装升级包;

步骤 S210、机顶盒安装下载的升级包。

本实施例中，升级服务设备针对不同的用户采用不同的加密密钥对升级包摘要加密，进一步增强了安全性，可避免在所有用户使用相同密钥时因密钥泄露而影响所有用户机顶盒软件升级的情况的发生。

图 3 所示实施例中的判断升级包摘要与解密结果是否相同的步骤也可由机顶盒来执行。在这种情况下，机顶盒不需向用户识别模块发送升级包摘要，用户识别模块在解密后需将解密结果发送至机顶盒，然后机顶盒就可判断从

升级服务设备下载的升级包与用户识别模块返回的解密结果是否相同，并进而根据判断结果选择是否安装升级包。

最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

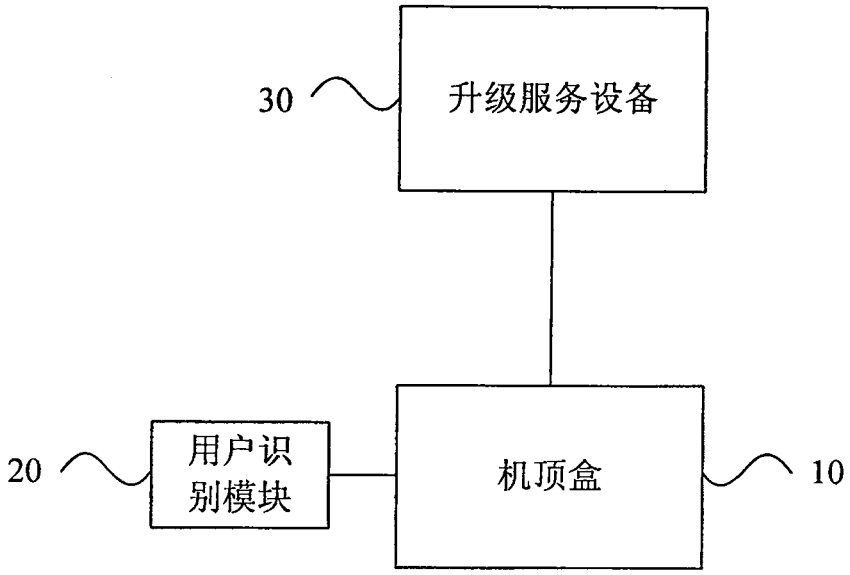


图 1

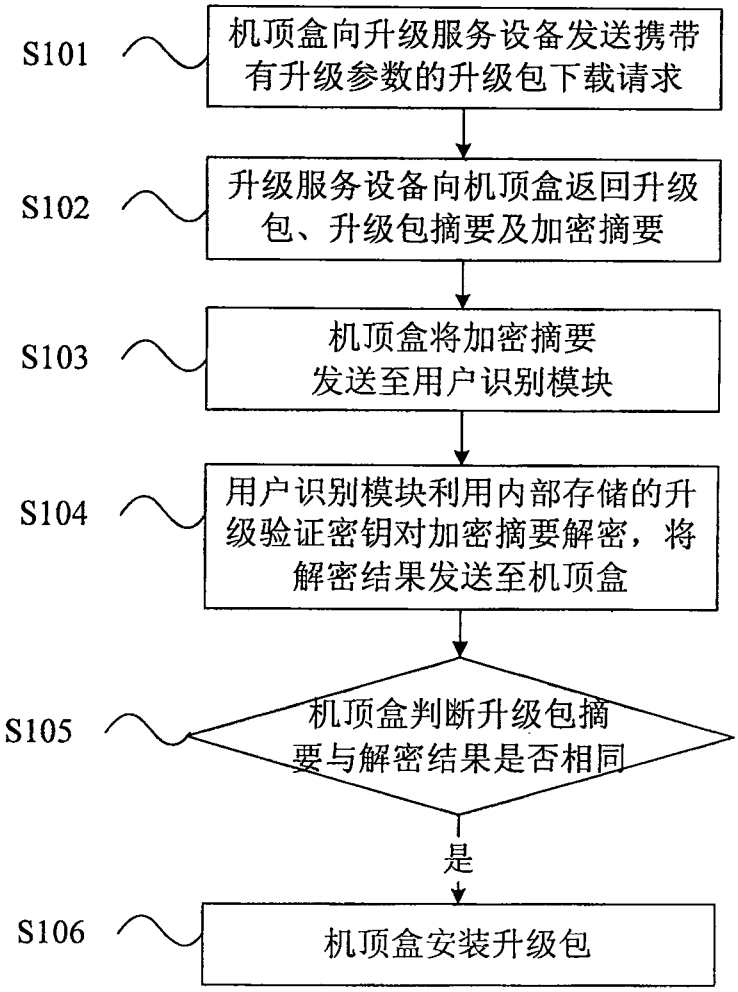

S101
机顶盒向升级服务设备发送携带有升级参数的升级包下载请求
S102
升级服务设备向机顶盒返回升级包、升级包摘要及加密摘要
S103
机顶盒将加密摘要发送至用户识别模块
S104
用户识别模块利用内部存储的升级验证密钥对加密摘要解密，将解密结果发送至机顶盒
S105
机顶盒判断升级包摘要与解密结果是否相同
是
S106
机顶盒安装升级包

图 2

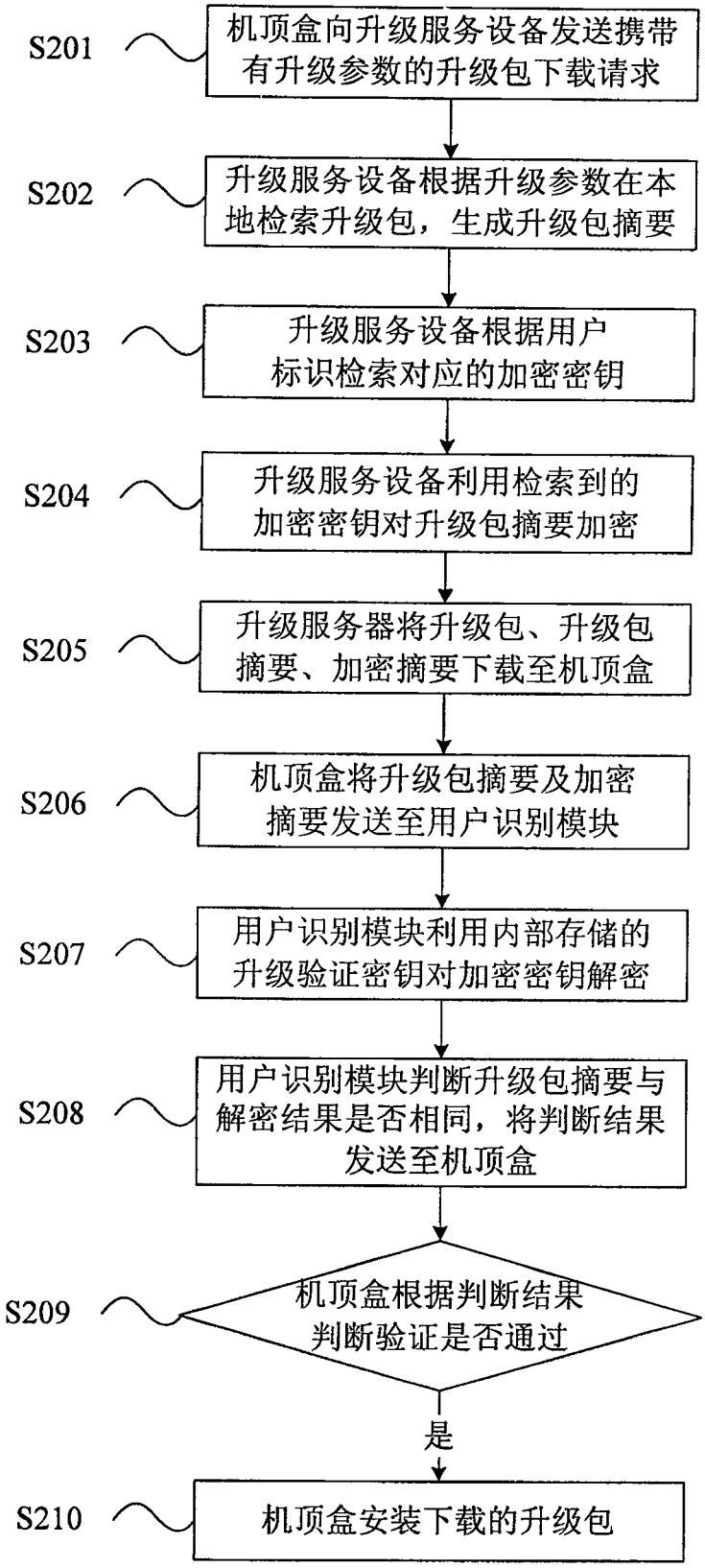

S201
机顶盒向升级服务设备发送携带有升级参数的升级包下载请求
S202
升级服务设备根据升级参数在本地检索升级包，生成升级包摘要
S203
升级服务设备根据用户标识检索对应的加密密钥
S204
升级服务设备利用检索到的加密密钥对升级包摘要加密
S205
升级服务器将升级包、升级包摘要、加密摘要下载至机顶盒
S206
机顶盒将升级包摘要及加密摘要发送至用户识别模块
S207
用户识别模块利用内部存储的升级验证密钥对加密密钥解密
S208
用户识别模块判断升级包摘要与解密结果是否相同，将判断结果发送至机顶盒
S209
机顶盒根据判断结果判断验证是否通过
是
S210
机顶盒安装下载的升级包

图 3