(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108123789 B
(45)授权公告日 2021.01.15

(21)申请号 201611063393.6
(22)申请日 2016.11.28
(65)同一申请的已公布的文献号
申请公布号 CN 108123789 A
(43)申请公布日 2018.06.05
(73)专利权人 中国移动通信有限公司研究院
地址 100053 北京市西城区宣武门西大街32号
专利权人 中国移动通信集团公司
(72)发明人 王峰生
(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静 刘伟
(51)Int.Cl.
H04L 9/00(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 101945109 A,2011.01.12
US 2016127908 A1,2016.05.05
审查员 刘莎莎

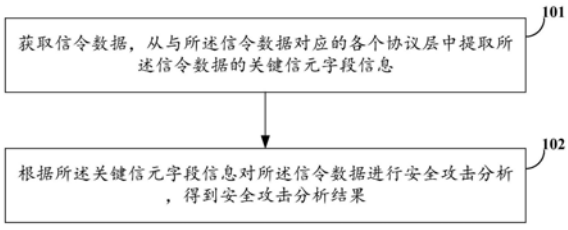
权利要求书2页 说明书10页 附图4页

(54)发明名称

分析安全攻击的方法及设备

(57)摘要

本发明实施例提供了一种分析安全攻击的方法及设备，该方法包括：获取信令数据，从与所述信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息；根据所述关键信元字段信息对所述信令数据进行安全攻击分析，得到安全攻击分析结果，解决现有技术中对于无防护手段的攻击，没有相应的方式实现对是否有无攻击或攻击成功与否的判断的问题。



CN 108123789 B

1.一种分析安全攻击的方法,其特征在于,包括:

获取信令数据,从与所述信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息;

根据所述关键信元字段信息对所述信令数据进行安全攻击分析,得到安全攻击分析结果,包括:

根据所述关键信元字段信息中的操作代码类型字段和消息方向字段,对所述信令数据进行分类,生成所述信令数据的分类检索信元数据文件,每种类型的分类检索信元数据文件包括该类型的请求方向文件和该类型的响应方向文件;

根据所述请求方向文件和响应方向文件对所述信令数据进行安全攻击分析,得到确认攻击集合和疑似攻击集合,包括:根据向内请求的原则,对分类检索信元数据文件中的请求方向文件进行过滤;

将符合过滤条件的请求方向文件中始源事务ID与响应方向文件中目的事务ID做关联检查;

如果请求方向文件中请求消息中始源事务ID和响应方向文件中响应消息中目的事务ID相同,并且在响应方向文件中响应消息中携带的位置信息字段显示为本国位置信息,则将请求消息和响应消息合并输出到与分类检索信元数据文件对应的确认攻击集合中;

如果没有与请求消息对应的响应消息,则将所述请求消息输出到与分类检索信元数据文件对应的疑似攻击集合中。

2.根据权利要求1所述的方法,其特征在于,所述获取信令数据,包括:

从国际关口局获取离线信令数据,所述离线信令数据是按照预定的时间间隔生成的数据包。

3.根据权利要求1所述的方法,其特征在于,根据向内请求的原则,对分类检索信元数据文件中的请求方向文件进行过滤,包括:

以目的信令点编码DPC为本国、始源信令点编码OPC为非本国、国际移动用户识别码IMSI或移动用户号码簿号码MDN为本国的过滤条件,对分类检索信元数据文件中的请求方向文件进行过滤。

4.一种分析安全攻击的设备,其特征在于,包括:

获取模块,用于获取信令数据,从与所述信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息;

分析模块,用于根据所述关键信元字段信息对所述信令数据进行安全攻击分析,得到安全攻击分析结果;

所述分析模块包括:

分类单元,用于根据所述关键信元字段信息中的操作代码类型字段和消息方向字段,对所述信令数据进行分类,生成所述信令数据的分类检索信元数据文件,每种类型的分类检索信元数据文件包括该类型的请求方向文件和该类型的响应方向文件;

分析单元,用于根据所述请求方向文件和响应方向文件对所述信令数据进行安全攻击分析,得到确认攻击集合和疑似攻击集合;

所述分析单元包括:

过滤子单元,用于根据向内请求的原则,对分类检索信元数据文件中的请求方向文件

进行过滤；

检查子单元，用于将符合过滤条件的请求方向文件中始源事务ID与响应方向文件中目的事务ID做关联检查；

如果请求方向文件中请求消息中始源事务ID和响应方向文件中响应消息中目的事务ID相同，并且在响应方向文件中响应消息中携带的位置信息字段显示为本国位置信息，则将请求消息和响应消息合并输出到与分类检索信元数据文件对应的确认攻击集合中；

如果没有与请求消息对应的响应消息，则将所述请求消息输出到与分类检索信元数据文件对应的疑似攻击集合中。

5.根据权利要求4所述的设备，其特征在于，所述获取模块包括：

获取单元，用于从国际关口局获取离线信令数据，所述离线信令数据是按照预定的时间间隔生成的数据包；

提取单元，用于从与所述离线信令数据对应的各个协议层中提取所述离线信令数据的关键信元字段信息。

6.根据权利要求4所述的设备，其特征在于，所述过滤子单元进一步用于：

以目的信令点编码DPC为本国、始源信令点编码OPC为非本国、国际移动用户识别码IMSI或移动用户号码簿号码MDN为本国的过滤条件，对分类检索信元数据文件中的请求方向文件进行过滤。

分析安全攻击的方法及设备

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种分析安全攻击的方法及设备。

背景技术

[0002] 近年来，随着传统GSM通信系统各项技术逐渐成熟，针对GSM系统中SS7信令安全的攻击报道和事件也日益增多，在这些大量的相关报道中常提及的安全威胁包括定位跟踪、呼叫转接、拒绝服务等。

[0003] 针对现有涉及SS7信令安全威胁的防护手段，主要通过信令防火墙根据信令GT码和携带的用户识别码(MDN或IMSI)加上单条信令指令行为特征进行判断，如果符合一定的异常行为特征，则认为属于安全威胁，进行相应防护动作。

[0004] 现有SS7信令安全防护手段可以见表1：

[0005] 表1SS7信令安全防护手段

[0006]

安全威胁	涉及信令	防护手段
定位跟踪	anyTimeInterrogation	符合源 GT 白名单放通，不符合拦截
	sendRoutingInfo	符合源 GT 或目的 GT 白名单放通，不符合拦截
	provideSubscriberInformation	发送消息网元和其查询用户匹配放通，不符合进行拦截
	provideSubscriberLocation	无防护手段
呼叫劫持	insertSubscriberData	无防护手段
拒绝服务	cancelLocation	无防护手段
	deleteSubscriberData	无防护手段

[0007]

[0008] 针对定位跟踪，存在部分防护手段，而对于呼叫劫持和拒绝服务类，则无具体防护手段；对于有防护手段的攻击，并无具体的审计方式、方法或系统、设备等对已实施防护手段进行核查，同样，对于无防护手段的攻击，也无相应的审计，来实现对是否有无攻击或攻击成功与否的判断。

发明内容

[0009] 鉴于上述技术问题，本发明实施例提供一种分析安全攻击的方法及设备，解决现有技术中对于无防护手段的攻击，没有相应的方式实现对是否有无攻击或攻击成功与否的判断的问题。

[0010] 本发明实施例的第一方面，提供了一种分析安全攻击的方法，包括：

[0011] 获取信令数据，从与所述信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息；

[0012] 根据所述关键信元字段信息对所述信令数据进行安全攻击分析，得到安全攻击分析结果。

[0013] 可选地，所述获取信令数据，包括：

[0014] 从国际关口局获取离线信令数据，所述离线信令数据是按照预定的时间间隔生成的数据包。

[0015] 可选地，根据所述关键信元字段信息对所述信令数据进行安全攻击分析，得到安全攻击分析结果，包括：

[0016] 根据所述关键信元字段信息中的操作代码类型字段和消息方向字段，对所述信令数据进行分类，生成所述信令数据的分类检索信元数据文件，每种类型的分类检索信元数据文件包括该类型的请求方向文件和该类型的响应方向文件；

[0017] 根据所述请求方向文件和响应方向文件对所述信令数据进行安全攻击分析，得到确认攻击集合和疑似攻击集合。

[0018] 可选地，所述根据所述请求方向文件和响应方向文件进行安全攻击分析，得到确认攻击集合和疑似攻击集合，包括：

[0019] 根据向内请求的原则，对分类检索信元数据文件中的请求方向文件进行过滤；

[0020] 将符合过滤条件的请求方向文件中始源事务ID与响应方向文件中目的事务ID做关联检查；

[0021] 如果请求方向文件中请求消息中始源事务ID和响应方向文件中响应消息中目的事务ID相同，并且在响应方向文件中响应消息中携带的位置信息字段显示为本国位置信息，则将请求消息和响应消息合并输出到与分类检索信元数据文件对应的确认攻击集合中；

[0022] 如果没有与请求消息对应的响应消息，则将所述请求消息输出到与分类检索信元数据文件对应的疑似攻击集合中。

[0023] 可选地，根据向内请求的原则，对分类检索信元数据文件中的请求方向文件进行过滤，包括：

[0024] 以目的信令点编码DPC为本国、始源信令点编码OPC为非本国、国际移动用户识别码IMSI或移动用户号码簿号码MDN为本国的过滤条件，对分类检索信元数据文件中的请求方向文件进行过滤。

[0025] 依据本发明实施例的第二个方面，还提供了一种分析安全攻击的设备，包括：

[0026] 获取模块，用于获取信令数据，从与所述信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息；

[0027] 分析模块，用于根据所述关键信元字段信息对所述信令数据进行安全攻击分析，

得到安全攻击分析结果。

[0028] 可选地，所述获取模块包括：

[0029] 获取单元，用于从国际关口局获取离线信令数据，所述离线信令数据是按照预定的时间间隔生成的数据包；

[0030] 提取单元，用于从与所述离线信令数据对应的各个协议层中提取所述离线信令数据的关键信元字段信息。

[0031] 可选地，所述分析模块包括：

[0032] 分类单元，用于根据所述关键信元字段信息中的操作代码类型字段和消息方向字段，对所述信令数据进行分类，生成所述信令数据的分类检索信元数据文件，每种类型的分类检索信元数据文件包括该类型的请求方向文件和该类型的响应方向文件；

[0033] 分析单元，用于根据所述请求方向文件和响应方向文件对所述信令数据进行安全攻击分析，得到确认攻击集合和疑似攻击集合。

[0034] 可选地，所述分析单元包括：

[0035] 过滤子单元，用于根据向内请求的原则，对分类检索信元数据文件中的请求方向文件进行过滤；

[0036] 检查子单元，用于将符合过滤条件的请求方向文件中始源事务ID与响应方向文件中目的事务ID做关联检查；

[0037] 如果请求方向文件中请求消息中始源事务ID和响应方向文件中响应消息中目的事务ID相同，并且在响应方向文件中响应消息中携带的位置信息字段显示为本国位置信息，则将请求消息和响应消息合并输出到与分类检索信元数据文件对应的确认攻击集合中；

[0038] 如果没有与请求消息对应的响应消息，则将所述请求消息输出到与分类检索信元数据文件对应的疑似攻击集合中。

[0039] 可选地，所述过滤子单元进一步用于：

[0040] 以目的信令点编码DPC为本国、始源信令点编码OPC为非本国、国际移动用户识别码IMSI或移动用户号码簿号码MDN为本国的过滤条件，对分类检索信元数据文件中的请求方向文件进行过滤。

[0041] 上述技术方案中的一个技术方案具有如下优点或有益效果：获取信令数据，从与信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息；然后根据关键信元字段信息对所述信令数据进行安全攻击分析，得到安全攻击分析结果，解决现有技术中对于无防护手段的攻击，没有相应的方式实现对是否有无攻击或攻击成功与否的判断的问题。现有方案重在拦截、防护，缺少对事后效果确认的手段，而本实施例能够得到该信令数据的安全攻击分析结果，提供了一种对事后效果确认的手段；进一步地，本实施例实现基于现网抓取数据，可从现有国际关口局信令监测数据中获取，不增加信令获取成本；而且本实施例可以为审计报告输出，不对现网产生立即影响；针对安全攻击分析结，现网可在后续酌情进行操作。

附图说明

[0042] 图1为本发明实施例一中分析安全攻击的方法的流程图；

[0043] 图2为本发明实施例一中攻击涉及7号信令各协议层的示意图；

[0044] 图3为本发明实施例一中步骤102的流程图；

[0045] 图4为本发明实施例一中步骤1022的流程图；

[0046] 图5为本发明实施例二中分析安全攻击的设备的框图之一；

[0047] 图6为本发明实施例二中分析安全攻击的设备的框图之二。

具体实施方式

[0048] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0049] 本领域技术人员知道，本发明的实施方式可以实现为一种系统、装置、设备、方法或计算机程序产品。因此，本发明的实施例可以具体实现为以下形式：完全的硬件、完全的软件(包括固件、驻留软件、微代码等)，或者硬件和软件结合的形式。

[0050] 实施例一

[0051] 参见图1，图中示出了一种分析安全攻击的方法，具体步骤如下：

[0052] 步骤101、获取信令数据，从与所述信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息；

[0053] 在本实施例中，可选地，从国际关口局获取离线信令数据，所述离线信令数据是按照预定的时间间隔生成的数据包。通过从现网国际关口局已建设信令相关系统中获取出、入双方向离线信令数据，无需对现网进行改造，不会对网络造成影响。上述离线信令数据可以为获取国际关口局双向数据，离线信令数据存储格式可以为PCAP文件，离线信令数据文件存储时长可以是预定的时间间隔(例如2分钟)生成一个数据包，离线信令数据文件名称格式可以为cvt_yyyymmddhhmiss.pcap；

[0054] 数据文件例如：cvt_20150207194922.pcap

[0055] 文件格式说明：

[0056] cvt-文件前缀

[0057] ‘_’-分隔符

[0058] yyyy-4位，代表年

[0059] mm-2位，代表月

[0060] dd-2位，代表日

[0061] hh-2位，代表时

[0062] mi-2位，代表分

[0063] ss-2位，代表秒

[0064] 以7号信令为例，与该7号信令对应的各个协议层如图2所示。

[0065] 同样，以7号信令为例，各层提取关键信元字段信息见下表：

[0066]

协议层	提取字段
MTP3	DPC、OPC
SCCP	CdPA GT、CdPA SSN 、CgPA GT、CgPA SSN
TCAP	MessageTypeTag、TransactionID
MAP	ComponentTypeTag、 InvokeID、 OperationCode、 IMSI/MDN、 LocationInformation、Ext-GeographicalInformation、 gsmSCF-Address

[0067] 步骤102、根据所述关键信元字段信息对所述信令数据进行安全攻击分析，得到安全攻击分析结果。

[0068] 参见图3，图中示出了步骤102的流程，具体步骤如下：

[0069] 步骤1021、根据所述关键信元字段信息中的操作代码类型字段和消息方向字段，对所述信令数据进行分类，生成所述信令数据的分类检索信元数据文件，每种类型的分类检索信元数据文件包括该类型的请求方向文件和该类型的响应方向文件；

[0070] 上述操作代码类型字段可以表示为OperationCode，包括：ati、sri、psi、psl、isd、cl、dsd。

[0071] 上述消息方向字段可以表示为ComponentTypeTag，包括：invoke代表向内请求，rr/rrnl代表向外响应。

[0072] 步骤1022、根据所述请求方向文件和响应方向文件对所述信令数据进行安全攻击分析，得到确认攻击集合和疑似攻击集合。

[0073] 进一步地，将按攻击类型区分的确认攻击列表和疑似攻击列表，整合输出。

[0074] 上述分类检索信元数据文件可以包括：定位跟踪分类检索信元数据表、呼叫劫持分类检索信元数据表和拒绝服务分类检索信元数据表，

[0075] 1)定位跟踪分类检索信元数据表文件名称格式如下：

[0076] OperationCode_ComponentTypeTag_离线信令数据文件名.txt

[0077] 定位跟踪分类检索信元数据表文件名如下：

[0078] ati_invoke_cvt_20150207194922.txt

[0079] ati_rr_cvt_20150207194922.txt

[0080] sri_invoke_cvt_20150207194922.txt

[0081] sri_rr_cvt_20150207194922.txt

[0082] sri_rrnl_cvt_20150207194922.txt

[0083] psi_invoke_cvt_20150207194922.txt

[0084] psi_rr_cvt_20150207194922.txt

[0085] psl_invoke_cvt_20150207194922.txt

[0086] psl_rr_cvt_20150207194922.txt

[0087] 其中，sri消息定位信息不仅存在于ReturnResult(Last)消息中，也存在LocationInformation和Ext-GeographicalInformation字段通过ReturnResult(NotLast)

消息返回的情况，需要对OperationCode为sri的消息补充输出sri_rrnl_cvt_20150207194922.txt。

[0088] 2)呼叫劫持分类检索信元数据表文件名称格式如下：

[0089] OperationCode_ComponentTypeTag_si_离线信令数据文件名.txt

[0090] OperationCode_ComponentTypeTag_si_gsmSCF_离线信令数据文件名.txt

[0091] OperationCode_ComponentTypeTag_gsmSCF_离线信令数据文件名.txt

[0092] OperationCode_ComponentTypeTag_离线信令数据文件名.txt

[0093] 呼叫劫持分类检索信元数据表文件名如下：

[0094] isd_invoke_si_cvt_20150207194922.txt

[0095] isd_invoke_si_gsmSCF_cvt_20150207194922.txt

[0096] isd_invoke_gsmSCF_cvt_20150207194922.txt

[0097] isd_rr_cvt_20150207194922.txt

[0098] 由于isd的invoke方向消息中存在：

[0099] 仅提供subscriberIdentity

[0100] 仅提供gsmSCF-Address

[0101] 提供subscriberIdentity和gsmSCF-Address，三种情况，需要在生成3类分类检索信元数据表文件。

[0102] 3)拒绝服务分类检索信元数据表文件名称格式如下：

[0103] OperationCode_ComponentTypeTag_离线信令数据文件名.txt

[0104] 拒绝服务分类检索信元数据表文件名如下：

[0105] cl_invoke_cvt_20150207194922.txt

[0106] cl_rr_cvt_20150207194922.txt

[0107] dsd_invoke_cvt_20150207194922.txt

[0108] dsd_rr_cvt_20150207194922.txt

[0109] 进一步地，在本实施例中，可以对定位跟踪分类检索信元数据表、呼叫劫持分类检索信元数据表和拒绝服务分类检索信元数据表中的消息进行去重处理，具体地，将定位跟踪分类检索信元数据表、呼叫劫持分类检索信元数据表和拒绝服务分类检索信元数据表中同类消息、相同方向文件合并，并将重传的同一条消息做去重检查，将完全相同的重传消息数据剔出，仅保留一条对应数据。

[0110] 经过上述处理后，把信令数据按消息类型、消息方向进行分类、合并、去重输出，作为后续特征分析处理的输入。处理后的文件名如下：

[0111] ati_invoke.txt/ati_rr.txt

[0112] sri_invoke.txt/sri_rr.txt/sri_rrnl.txt

[0113] psi_invoke.txt/psi_rr.txt

[0114] psl_invoke.txt/psl_rr.txt

[0115] isd_invoke_si.txt/isd_invoke_si_gsmSCF.txt/isd_invoke_gsmSCF.txt/isd_rr.txt

[0116] cl_invoke.txt/cl_rr.txt

[0117] dsd_invoke.txt/dsd_rr.txt

[0118] 参见图4,图中示出了步骤1022的流程,具体步骤如下:

[0119] 步骤10221、根据向内请求的原则,对分类检索信元数据文件中的请求方向文件进行过滤;

[0120] 具体地,以目的信令点编码(DPC)为本国、始源信令点编码(OPC)为非本国、(国际移动用户识别码)IMSI或(移动用户号码簿号码)MDN为本国的过滤条件,对分类检索信元数据文件中的请求方向文件进行过滤。

[0121] 步骤10222、将符合过滤条件的请求方向文件中始源事务ID(OriginatingTransactionID)与响应方向文件中目的事务ID(DestinationTransactionID)做关联检查;

[0122] 步骤10223、如果请求方向文件中请求消息中始源事务ID和响应方向文件中响应消息中目的事务ID相同,并且在响应方向文件中响应消息中携带的位置信息字段(LocationInformation或者Ext-GeographicalInformation)显示为本国位置信息,则将请求消息和响应消息合并输出到与分类检索信元数据文件对应的确认攻击集合中;

[0123] 步骤10224、如果没有与请求消息对应的响应消息,则将所述请求消息输出到与分类检索信元数据文件对应的疑似攻击集合中。

[0124] 下面针对定位跟踪、呼叫劫持和拒绝服务三种安全威胁来描述如何得到安全分析结果。

[0125] 1)定位跟踪特征分析

[0126] 在定位跟踪分类检索信元数据表中,从请求方向invoke文件中,根据DPC为本国、OPC为非本国、IMSI或MDN为本国的过滤条件;将符合过滤条件的OriginatingTransactionID与响应方向rr或rrnl文件中DestinationTransactionID做关联检查,如果请求消息中OriginatingTransactionID和响应消息中DestinationTransactionID相同,并且在响应消息中携带的LocationInformation字段显示为本国位置信息,或在响应消息中携带的Ext-GeographicalInformation字段显示为本国位置信息,将请求消息和响应消息合并输出到确认定位跟踪攻击列表中;将有请求消息、无对应响应消息输出到疑似定位跟踪攻击列表中。

[0127] 2)呼叫劫持特征分析

[0128] 在呼叫劫持分类检索信元数据表中,从请求方向invoke文件中,先将仅提供subscriberIdentity和仅提供gsmSCF-Address的两个数据表根据OriginatingTransactionID字段做关联检查,如果两个表中存在OriginatingTransactionID字段相同的数据,将字段相同的两条数据合并追加到提供subscriberIdentity和gsmSCF-Address的数据表文件中。

[0129] 将整合后的提供subscriberIdentity和gsmSCF-Address的数据表文件中请求方向invoke消息,根据DPC为本国、OPC为非本国、IMSI或MDN为本国的过滤条件;将符合过滤条件的OriginatingTransactionID与响应方向rr文件中DestinationTransactionID做关联检查,如果请求消息中OriginatingTransactionID和响应消息中DestinationTransactionID相同,将请求消息和响应消息合并输出到确认呼叫劫持攻击列表中;将有请求消息,但无对应响应消息输出到疑似呼叫劫持攻击列表中。

[0130] 3)拒绝服务特征分析

[0131] 在拒绝服务分类检索信元数据表中，从请求方向invoke文件中，根据DPC为本国、OPC为非本国、IMSI或MDN为本国的过滤条件；将符合过滤条件的OriginatingTransactionID与响应方向rr文件中DestinationTransactionID做关联检查，如果请求消息中OriginatingTransactionID和响应消息中DestinationTransactionID相同，将请求消息和响应消息合并输出到确认拒绝服务攻击列表中；将有请求消息，但无对应响应消息输出到疑似拒绝服务攻击列表中。

[0132] 在本实施例中，首先获取信令数据，从与信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息；然后根据关键信元字段信息对所述信令数据进行安全攻击分析，得到安全攻击分析结果，解决现有技术中对于无防护手段的攻击，没有相应的方式实现对是否有无攻击或攻击成功与否的判断的问题。现有方案重在拦截、防护，缺少对事后效果确认的手段，而本实施例能够得到该信令数据的安全攻击分析结果，提供了一种对事后效果确认的手段；进一步地，本实施例实现基于现网抓取数据，可从现有国际关口局信令监测数据中获取，不增加信令获取成本；而且本实施例可以为审计报告输出，不对现网产生立即影响；针对安全攻击分析结，现网可在后续酌情进行操作。

[0133] 实施例二

[0134] 参见图5，图中示出了一种分析安全攻击的设备，该设备500包括：

[0135] 获取模块501，用于获取信令数据，从与所述信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息；

[0136] 在本实施例中，可选地，获取模块501从国际关口局获取离线信令数据，所述离线信令数据是按照预定的时间间隔生成的数据包。通过从现网国际关口局已建设信令相关系统中获取出、入双方向离线信令数据，无需对现网进行改造，不会对网络造成影响。

[0137] 分析模块502，用于根据所述关键信元字段信息对所述信令数据进行安全攻击分析，得到安全攻击分析结果。

[0138] 上述分析结果可以包括：确认定位跟踪攻击列表、疑似定位跟踪攻击列表、确认呼叫劫持攻击列表、疑似呼叫劫持攻击列表、确认拒绝服务攻击列表和疑似拒绝服务攻击列表。

[0139] 在本实施例中，可选地，所述获取模块501包括：获取单元5011和提取单元5012，参见图6，其中，

[0140] 获取单元5011，用于从国际关口局获取离线信令数据，所述离线信令数据是按照预定的时间间隔生成的数据包；

[0141] 提取单元5012，用于从与所述离线信令数据对应的各个协议层中提取所述离线信令数据的关键信元字段信息。

[0142] 在本实施例中，可选地，所述分析模块502包括：

[0143] 分类单元5021，用于根据所述关键信元字段信息中的操作代码类型字段和消息方向字段，对所述信令数据进行分类，生成所述信令数据的分类检索信元数据文件，每种类型的分类检索信元数据文件包括该类型的请求方向文件和该类型的响应方向文件；

[0144] 分析单元5022，用于根据所述请求方向文件和响应方向文件对所述信令数据进行安全攻击分析，得到确认攻击集合和疑似攻击集合。

[0145] 在本实施例中，可选地，所述分析单元5022包括：

[0146] 过滤子单元50221，用于根据向内请求的原则，对分类检索信元数据文件中的请求方向文件进行过滤；

[0147] 检查子单元50222，用于将符合过滤条件的请求方向文件中始源事务ID与响应方向文件中目的事务ID做关联检查；

[0148] 如果请求方向文件中请求消息中始源事务ID和响应方向文件中响应消息中目的事务ID相同，并且在响应方向文件中响应消息中携带的位置信息字段显示为本国位置信息，则将请求消息和响应消息合并输出到与分类检索信元数据文件对应的确认攻击集合中；

[0149] 如果没有与请求消息对应的响应消息，则将所述请求消息输出到与分类检索信元数据文件对应的疑似攻击集合中。

[0150] 在本实施例中，可选地，所述过滤子单元50221进一步用于：

[0151] 以目的信令点编码DPC为本国、始源信令点编码OPC为非本国、国际移动用户识别码IMSI或移动用户号码簿号码MDN为本国的过滤条件，对分类检索信元数据文件中的请求方向文件进行过滤。

[0152] 在本实施例中，首先获取信令数据，从与信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息；然后根据关键信元字段信息对所述信令数据进行安全攻击分析，得到安全攻击分析结果，解决现有技术中对于无防护手段的攻击，没有相应的方式实现对是否有无攻击或攻击成功与否的判断的问题。现有方案重在拦截、防护，缺少对事后效果确认的手段，而本实施例能够得到该信令数据的安全攻击分析结果，提供了一种对事后效果确认的手段；进一步地，本实施例实现基于现网抓取数据，可从现有国际关口局信令监测数据中获取，不增加信令获取成本；而且本实施例可以为审计报告输出，不对现网产生立即影响；针对安全攻击分析结，现网可在后续酌情进行操作。

[0153] 应理解，说明书通篇中提到的“一个实施例”或“一实施例”意味着与实施例有关的特定特征、结构或特性包括在本发明的至少一个实施例中。因此，在整个说明书各处出现的“在一个实施例中”或“在一实施例中”未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。

[0154] 在本发明的各种实施例中，应理解，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定

[0155] 另外，本文中术语“系统”和“网络”在本文中常可互换使用。

[0156] 应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0157] 在本申请所提供的实施例中，应理解，“与A相应的B”表示B与A相关联，根据A可以确定B。但还应理解，根据A确定B并不意味着仅仅根据A确定B，还可以根据A和/或其它信息确定B。

[0158] 在本申请所提供的几个实施例中，应该理解到，所揭露方法和装置，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合

或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0159] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理包括，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0160] 上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述收发方法的部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(Read-Only Memory，简称ROM)、随机存取存储器(Random Access Memory，简称RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0161] 以上所述的是本发明的优选实施方式，应当指出对于本技术领域的普通人员来说，在不脱离本发明所述的原理前提下还可以做出若干改进和润饰，这些改进和润饰也在本发明的保护范围内。

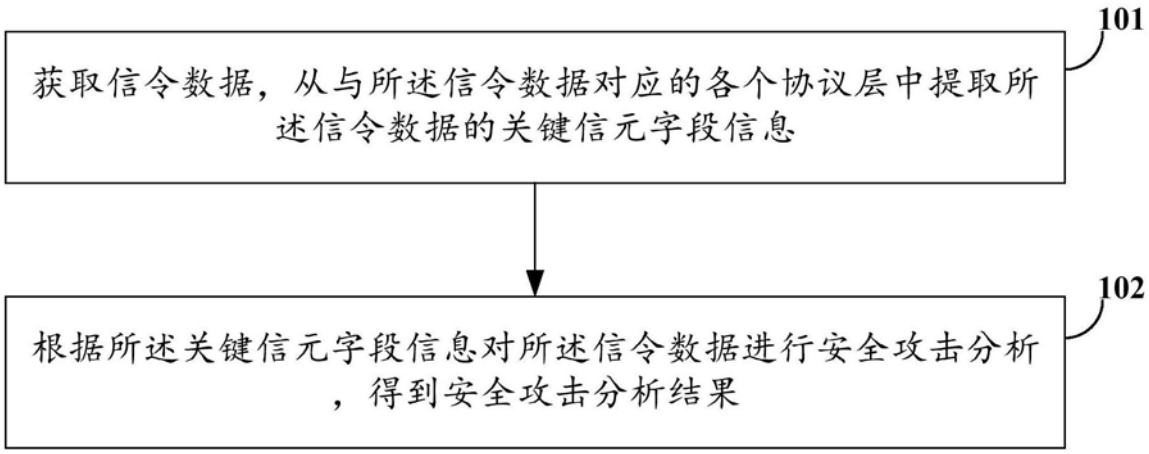

101
获取信令数据，从与所述信令数据对应的各个协议层中提取所述信令数据的关键信元字段信息
102
根据所述关键信元字段信息对所述信令数据进行安全攻击分析，得到安全攻击分析结果

图1


MAP
TCAP
SCCP
MTP3

图2

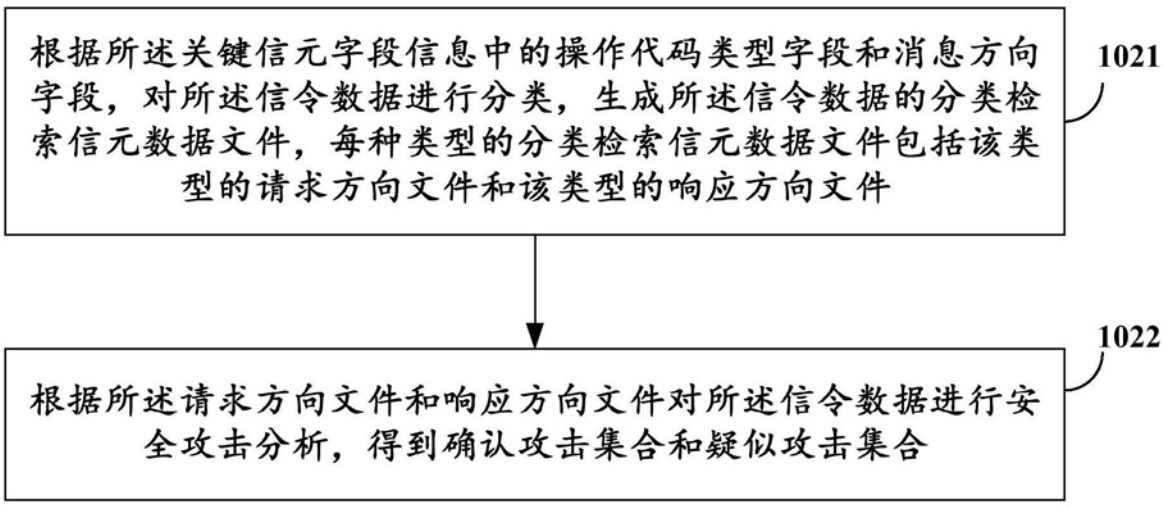

根据所述关键信元字段信息中的操作代码类型字段和消息方向字段，对所述信令数据进行分类，生成所述信令数据的分类检索信元数据文件，每种类型的分类检索信元数据文件包括该类型的请求方向文件和该类型的响应方向文件
1021
根据所述请求方向文件和响应方向文件对所述信令数据进行安全攻击分析，得到确认攻击集合和疑似攻击集合
1022

图3

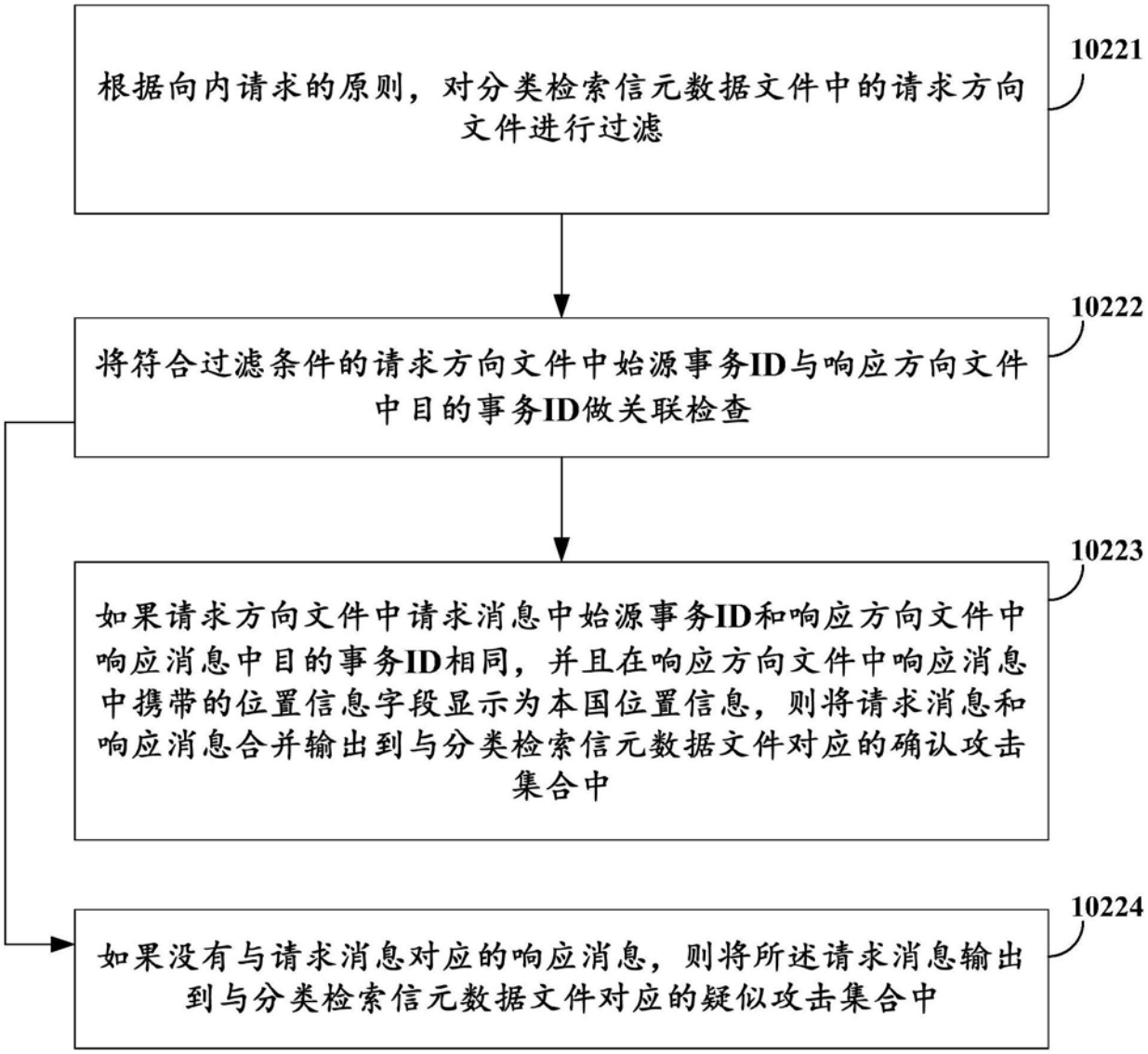

根据向内请求的原则，对分类检索信元数据文件中的请求方向文件进行过滤
10221
将符合过滤条件的请求方向文件中始源事务ID与响应方向文件中目的事务ID做关联检查
10222
如果请求方向文件中请求消息中始源事务ID和响应方向文件中响应消息中目的事务ID相同，并且在响应方向文件中响应消息中携带的位置信息字段显示为本国位置信息，则将请求消息和响应消息合并输出到与分类检索信元数据文件对应的确认攻击集合中
10223
如果没有与请求消息对应的响应消息，则将所述请求消息输出到与分类检索信元数据文件对应的疑似攻击集合中
10224

图4

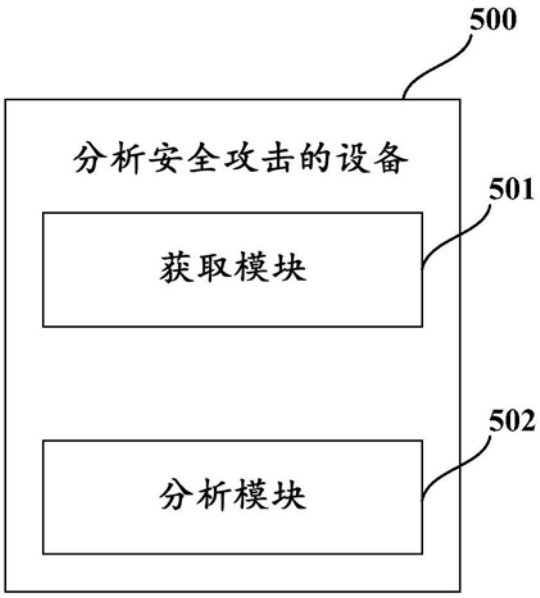


图5

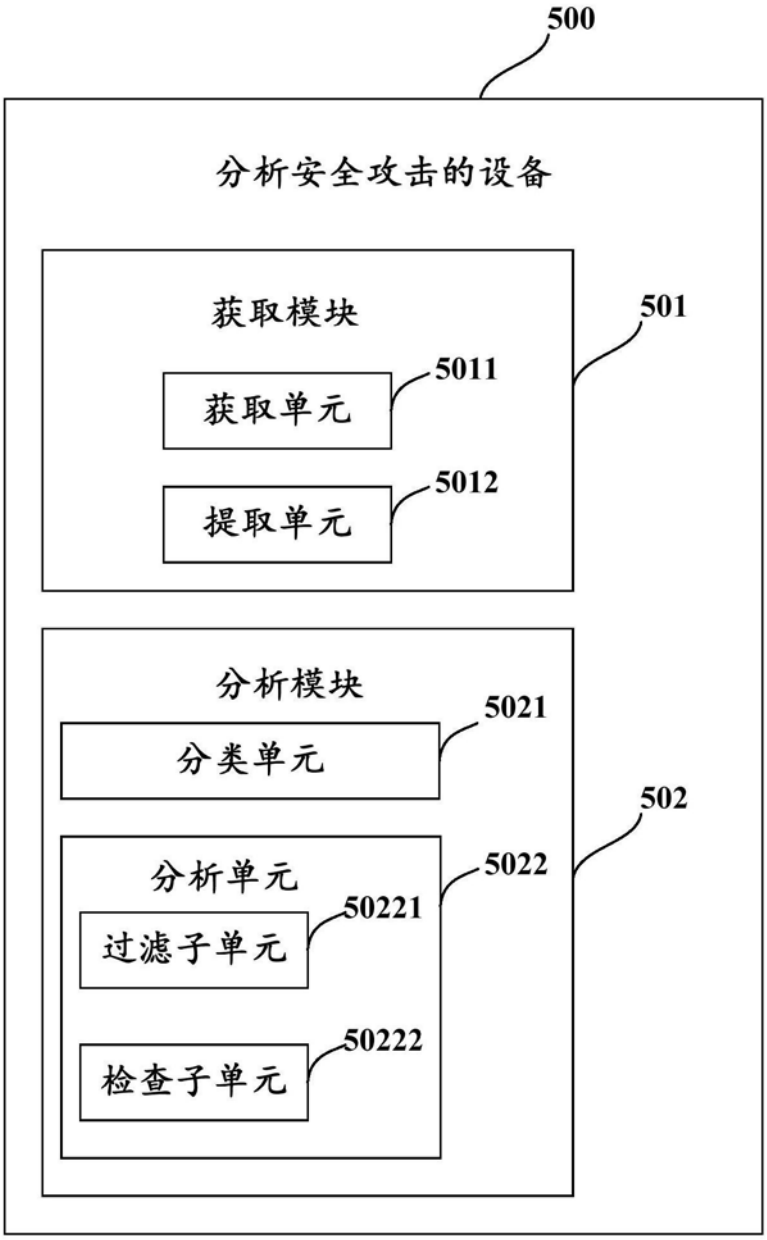

500
分析安全攻击的设备
获取模块
501
5011
获取单元
5012
提取单元
分析模块
5021
分类单元
502
分析单元
5022
50221
过滤子单元
50222
检查子单元

图6