IKEv2加密破碎PQ 认证的安全分析

rfc7383 — ProVerif+ 代理 报告

文稿	互联网密钥交换协议版本2(IKEv2)消息断裂(协议定义)); 互联网密钥交换协议版本2(IKEv2) (辅助))
检查的性质	13 条：13 条成立，0 条不成立
发现	2

目录

1 协议和范围

2 发现

3 检查过的性质

4 本次分析的局限

附录 A：逐条性质的解读

附录 C：主张和证明器的答案

附录 D：分析是怎么跑的

1 协议和范围

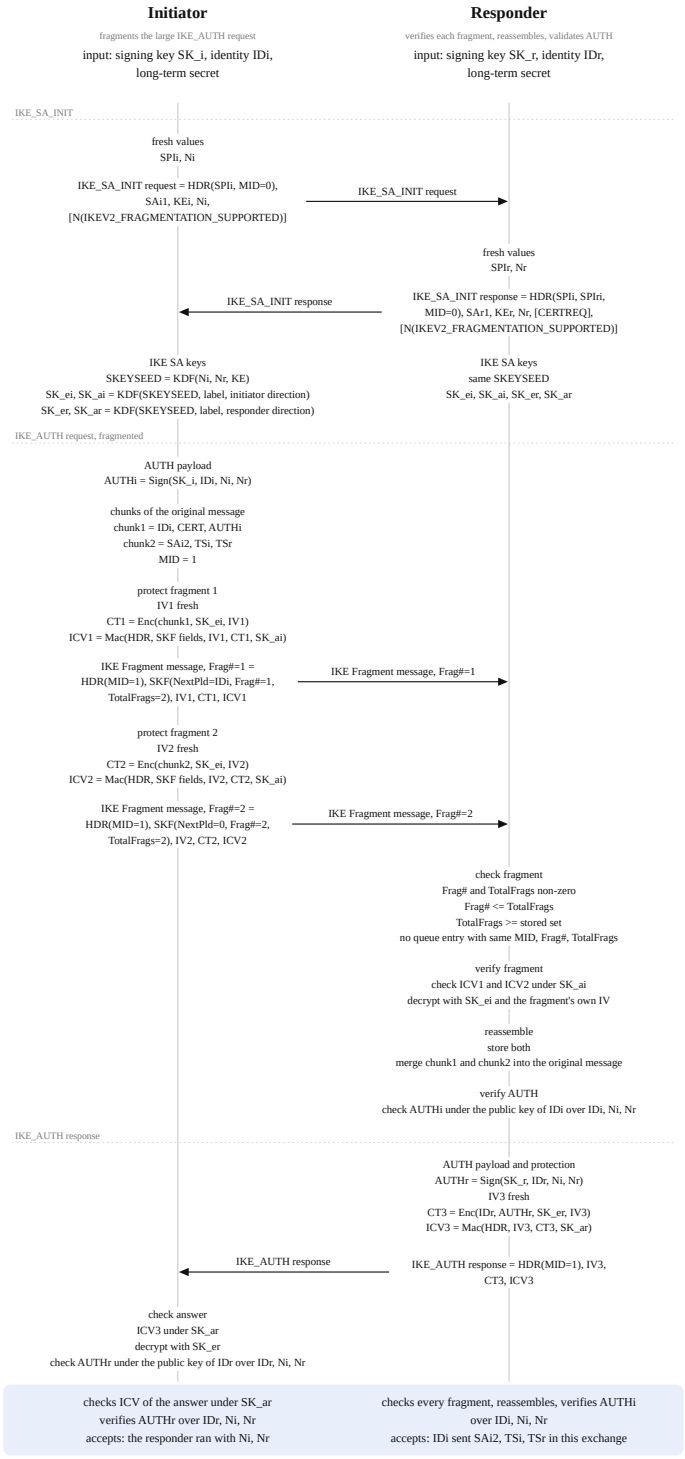
RFC 7383 让两个IKEv2同伴发出一个对于路径来说太大的信息,作为IKE个碎片信息系列,而不是IP个碎片. 这对IKE_AUTH来说最为重要,在那里,一个大型的量子后签名及其证书可以将一个消息推过MTU的路径. 发起人持有其签名密钥和身份,响应者持有自己的身份,两者都持有IKE SA密钥所衍生的长期秘密.

IKE_AUTH的信息在加密前是零碎的,因此每个片段都是加密的,完整性是自己保护的,并携带自己的初始化矢量. 双方持有两方向的IKE SA键,Message ID计数器,在接收方则持有重新组装的队列. 当交换结束时,应答者确定哪个发起者身份证明了其AUTH有效载荷在本次交换的非ces上,并随即收到了SA的数据,应答者也以同样的方式肯定了应答者.

双方:

- **发起者**:将IKE_AUTH项大型请求碎裂。 持有:签署密钥SK_i,身份IDi,长期保密.
- **反应器**:核实每个碎片,重新组装,验证AUTH。 持有:签署密钥SK_r,身份IDr,长期保密.

图1显示交易所,如文件所示。



- 图1。 指定协议 。 *

分析的范围载于附录D:分析的内容、遗漏的内容和文件的章节。

2 发现

分析有2项调查结果:以下内容没有在文件中说明。 对于其中的2人,不清楚这些文件是否说明了他们。

在所分析的范围内,RFC 7383破碎提供了它要给予的:13个被检查者的财产都没有对网络攻击者失败. 每个碎片都是真实的,并捆绑在它的IKE SA,方向,訊息ID,裂片编号和总裂片,不同套件的片段从未合并过,只有经过彻底重新组装后才会解析该信息,AUTH有效载荷在采取行动前通过该交换机的非切片进行验证. 与接收器一起检查了碎片集的重新播放、再传输处理和初始化矢量新鲜度,发送器没有卷到三个碎片到达处,它们也在那里停留。 所报道的文档写下的内容有两个漏洞,而不是模型中的攻击,即接收方的重播测试没有指定方向,对重复的第一个碎片的授权回答告诉攻击者,请求已经处理. 结果没有涵盖的是IKE_SA_INIT的关键协议,资源耗尽攻击文件本身所述的,以及原始人的力量.

2.1重播测试RFC7383不指定方向, 因此一个队列服务于两个方向

类型	协议规范本身的弱点
是否新发现	不确定：文稿只写了一部分，或没能检索
价值	中
涉及的性质	U01, R02, A08 （见第 3 节）
原文	s0031, s0040, s0077, s0087, s0110

发生了什么。 接收方通过将ID号信件、碎片编号和到达碎片的总碎片与其队列中的碎片进行比较来检测重播。 在一个IKE SA两个方向中,两个方向可能使用相同的Message ID值,每个整数可能出现在四个只有发起人和反应人旗帜区分的截然不同的电文中. 因此,一个为IKE SA号机保持一个队列的接收器将两个方向的片段通过不区分的字段进行比较. 分离完全取决于每块碎片的完整性检查值和每个方向的单独的完整性密钥,因为带有旗帜的头部在每一个碎片中行驶完好,并被该检查覆盖. 州检记录步骤,模式显示没有交叉方向接受,所以这是规则上的漏洞,而不是攻击.

攻击者需要什么。 书面文件之外没有其他文件:空白在规则中,不是攻击者的能力. 攻击需要一个在碎片匹配队列后检查其完整性的接收器,或者一个对双向使用单一完整性密钥的接收器.

攻击者能得到什么。 如果执行过其中之一,则可以将响应者请求的片段带入发起者请求的队列中,其信息内容相同:ID,破碎编号和总破碎,两组可以混合. 通过文件放置处的完整性检查,碎片不会通过,混合不会发生,模型证实了这一点.

拟议修改。 命名2.6节重播测试中的方向:一个片段是当队列持有一个与ID相同的条目,断裂号,总断裂和启动器旗时的重播,并声明每个方向的队列是分开的,这样规则就不会依赖检查的顺序.

用 ProVerif 复核。 未检查:该型号已经检查了每个碎片的方向,每IKE SA只持有一个零碎的请求,因此从型号上删除检查无法产生痕迹; 更改是规则的文本,经核实的交叉方向查询是检查是包含分离内容的证据.

2.2 对重复的第一个碎片的所需答复告诉攻击者是否处理了请求

类型	协议规范本身的弱点
是否新发现	不确定：文稿只写了一部分，或没能检索
价值	低
涉及的性质	S02, R02 （见第 3 节）
原文	s0076, s0078, s0088

发生了什么。 已经处理的请求的一个重复部分以两种不同的方式得到答复:用1号碎片,它触发了反应的再发送,而其他任何碎片号则被忽略。 所有其他拒绝都是沉默的。 因此,传送请求碎片的随路攻击者可以再次发送1碎片,并从重新发送的答复中了解答复者是否已经处理过请求,并从沉默中得知它没有处理过请求。 未滚动的接收器显示重传的答案是可到达的,两个答案是不同的.

攻击者需要什么。 攻击者必须在路径上,必须持有通过请求完整性检查的碎片,通过转发原始碎片获得; 没有别的了。

攻击者能得到什么。 攻击者了解一项请求的处理状态。IKESA它已经在处理。 它无法了解它没有看到的任何请求,也无法使答复者接受两次请求。

拟议修改。 无任何建议:反应的重传是使交换从丢失的响应中恢复的原因,任何消除差异的规则也消除了这种恢复. 想要清除漏水的编辑者必须定义每个重复的片段的统一答案.

用 ProVerif 复核。 未检查:规则的改变消除了文件要求的再发送回收,而模型不能对泄漏进行权衡; 没有改变信息或支票来保持两者。

3 检查过的性质

每行是一块财产,投入到ProVerif. 结果是ProVerif对分析师的协议模型的回答; 价值以及文件是否已经说明结果是分析员的判断,理由见附录A。

ID	性质	假定的泄露	结果	价值	文稿是否已写
A03	**重新组装后达成IKE_AUTH协议。** 每当接收方接受重组后的 IKE_AUTH（认证成功），都存在一个对端真实运行，角色、双方意图身份与协商数据一致。	无	成立	中	是
A04	**每个发起人接受一次。** 每次接收方接受重组后的 IKE_AUTH，都对应一个不同的对端真实运行（单射匹配），同一运行不能被接受两次。	无	成立	中	是
D01	**个别碎片的真实性和绑定性。** 每次接受一个 IKE分片（ICV校验通过），其受保护内容与上下文（消息ID、方向、碎块编号,总碎块数).都对应允许发送方的真实发送，未被篡改。	无	成立	高	是
R02	**不重放碎片集成员。** 在单个 IKESA范围内，同一 (减:ID,碎片数,共计碎片数).的分片至多被接受一次，重复到达必须被丢弃。	无	在一个约束内持有(变化中的数值未滚动到3步)	中	是
A08	**重新组合确定一致性。** 重组成功时，所有分片的 消息ID、方向、残块共计一致，断裂数覆盖 1. . 共计且不重复，下一个有效载荷只在第一片非零；不同集合的分片不会被混合。	无	成立	中	是
K01	**IKE SA密钥和IKE_AUTH内容密钥.** 攻击者不能推导出 SK_ei、SK_er、SK_ai、SK_ar 以及由它们保护的 IKE_AUTH 内容。	无	成立	中	是
K04	**每个方向分离密钥。** 发起方方向与响应方方向使用的加密与完整性密钥不同，不同 IKE SA 会话的密钥也不同。	无	成立	低	是
S01	**单键下无IV再利用。** 在同一真实密钥下，每次加密调用使用的完整 nonce(IV)不重复，包括重传不视为新加密。	无	在一个约束内持有(变化中的数值未滚动到3步)	低	是
S02	**重播处理不回滚状态。** 重传或重复分片的处理不会回退已安装密钥、清空接收窗口或恢复旧权限；仅 破碎编号为为 1 的重传可触发响应重传。	无	在一个约束内持有(变化中的数值未滚动到3步)	中	是
U01	**不将碎片搅拌到各组之间。** 不存在接收方接受重组 IKE_AUTH 而其分片来自不同 新闻 ID 或不同方向的轨迹。	无	成立	高	是
U02	**完全重新组装前不接受。** 不存在接收方在未完成全部分片校验前接受 IKE_AUTH 的轨迹。	无	成立	中	是
U03	**AUTH00美元在验收前已经核实。** 不存在接收方在未通过原始 IKE_AUTH 身份验证的情况下接受重组消息的轨迹。	无	成立	高	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
X01	**给发起人的对应认证。** 只有在答复者将答复真正寄出于同一非记录和身份时,发起者才接受IKE_AUTH份答复; 网络上的任何攻击者都不可能得到IKE_AUTH的响应,没有这样的运行。	无	成立	中	是

文稿写明而起草的清单里没有、由分析者补充的目标（见附录 D）：X01.

所问之问,及分析师之答:

问题	回答	依据
Q1: 不同消息/方向的加密分片不能拼接成成功 IKE_AUTH	没有痕量将不同信息IDs的碎片或不同方向的碎片合并为接受的IKE_AUTH:接受信息的两个碎片都是按照该信息ID发出的,并带有相同的完全碎片。 写成的重播规则没有给方向命名,因此分离通过perflagment完整性检查和单独的密钥来进行,这些密钥被报告为文本中的漏洞而不是攻击.	U01, A08, D01
Q2: 篡改/重复/缺片不会在未完整验证前被接受	坦佩雷,重播或缺失的片段并不能导致接受:一个片段未能完成完整性检查或其数字测试从未进入队列,一个重复的片段被丢弃或只引发存储的答案的重播,消息被解析,只有在完整集收到并合并后才采取行动.	U02, R02, S02, D01
Q3: 重组成功依然需要原始 IKE_AUTH 身份验证	成功重新组装仍需要原始认证:接受的IKE_AUTH总是带有声称身份的签名,上面写着这个交换机的非ces,以及该身份,在信息被执行之前经过核实,所以重新组装不会让任何东西越过AUTH有效载荷.	U03, A03

4 本次分析的局限

这里的一个结果就是协议模型的结果:它描述了特定的信息和检查给出的或未能给出的,以密码学为理想,没有关于执行的内容.

正如分析师所说,这一分析没有涵盖的内容是:

- IKE_SA_INIT的关键协议不是模型化的:IKE SA的密钥来源于同龄人共享的一个长期秘密,因此远期保密,协议的强度以及完成IKE_SA_INIT而不经过认证的攻击者都不属于这些结果.
- 该电文被固定为1和2号断裂片的2个碎片中的1个零碎IKE_AUTH; 更多的碎片, PMTU的发现 改变 Total Flagments, 和规则 一个更大的 Total Flagments 重启 重新组装没有被执行。
- 资源耗尽的攻击文件状态(一个完成IKE_SA_INIT并且向重装缓冲器中发送大量但不完整的碎片的攻击者)并不是模拟的:证明器不问内存或碎片计数,攻击者在其中持有它自己的IKE SA的密钥,这个模型来源于它无法计算的秘密.
- 重新组装超时、重新传输计时器和重新传输的次数没有模型化; 只有接收者在到达之间保持状态,没有卷到3个。
- 签名的octets的长度缩小为两个非ces和身份; 其余的有效载荷由IKE SA号的完整密钥保护,但其内容是单一常数。
- 原始人的力量是假设的:签名是不可原谅的,完整性检查是理想的MAC,加密是没有代数属性的构造器-破坏器对. 关于量子后安全等级,SLH-DSA的签名-计数限额,或PQC认证文件所述的对算法谈判的降级攻击,都没有任何说法.
- IKE分解支持的谈判,算法谈判,EAP认证,重键,NAT转盘和流量选择器的授权均不在模型之外.

主持人记录的是什么:

- A04,R02,A08,S01,S02,U02的回答,都停留在简化型号的操作上(附录D).
- 没带对照查询的证明（附录 C):A04:邦斯,R02:邦斯,A08:邦斯,K01:k01_key,K04:k04,S01:biv,S02:邦斯. 对照查询是这条性质的一个必然不成立的变体；没有它，就没有东西表明这条性质照现在的写法在模型里有可能不成立。

附录A中列出了每个财产的开口情况以及解决这些财产的办法。

附录 A：逐条性质的解读

分析师自己对证明器的答案的解读,而不是对证明器的答案:答案对协议的意义,读取的基础,是否可以按原样使用,价值如何.

A03:IKE_AUTH 重新组装后的协议

每当接收方接受重组后的 IKE_AUTH（认证成功），都存在一个对端真实运行，角色、双方意图身份与协商数据一致。

接受重新组装的IKE_AUTH总是符合IKE SA的发起人的真实运行,同时具有相同的Message ID,相同的身份,相同的要求的响应者身份,相同的SA数据以及相同的两个非C. 网络上的攻击者不能得到发起者没有发出的信息的接受,因为碎片内容用方向的密钥加以保护,AUTH有效载荷是针对发起者身份和双非的签名.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:它确认在碎裂后交换的中心保证; 值受理想化关键协议的限制。
- 在文件中说明:是的。 文件中说:rfc7296:585,主:624
- 休息:IKE SA的密钥来源于一个长期共享的秘密,而不是迪菲-赫尔曼或IKE_SA_INIT协议的PQ-KEM,因此IKE SA的密钥的密钥就在于这个秘密; 签名的octets被简化为两个非ces和身份; SA数据由IKE SA的完整密钥保护,而不是由签字保护; a. 每IKE SA发2个碎片的零碎信息; 请求区采用单一SA有效载荷常数的模型
- 打开:答复者接受不同情况的情况IDr而不是所要求的一个模型是不受限制的,因为rfc7296允许
- 下一步:模拟迪菲-赫尔曼IKE_SA_INIT与Tamarin+ Agent的交换,去除共享机密的理想化.

A04:每个发起人一次验收

每次接收方接受重组后的 IKE_AUTH，都对应一个不同的对端真实运行（单射匹配），同一运行不能被接受两次。

每次接受都与不同的发起者运行相匹配:一次又一次接受请求。 由于接收器没有卷进三个碎片到达,当接受请求的碎片被重新播放时,就会留下,因为重复的碎片被丢掉,只有存储的答案被重新传送。

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:它显示重传和重播规则使请求无法被两次接受,这就是ID和片段数逻辑的目的.
- 在文件中说明:是的。 文件中说:rfc7296:108,主:669
- 休息:在模型中每IKESA个零碎请求。 pv; (中文(简体)). 重播案件只包含在未滚动的界限内。 pv至3名抵达者; 重放检查是接收者在队列中保存的检查:存储碎片的设定身份和请求得到处理的事实
- 打开:超过3个到达者,以及排队的超时,不是不滚动的
- 下一步:进一步翻转或模拟定时器以覆盖更长的离合时间.

D01: 单个碎片的真实性和装订

每次接受一个 IKE 分片（ICV 校验通过），其受保护内容与上下文（ 信号 ID 方向、 裂痕编号,总裂痕) 都对应允许发送方的真实发送，未被篡改。

接收器接收的每个碎片都是由IKE SA的发起人按收到时的准确顺序发送的,其信息内容与ID,碎片编号,碎片总数和内容相同. 任何为另外IKE SA而修改,伪造或保护的事物,或者其他方向都失败了完整性检查,从不进入队列,这就是文件将伪造的碎片保存在重新组装缓冲器之外所依赖的财产.

- 结果:持有; 回答问题:是的; 可用
- 高值:这是扩展所要存在的每块碎片的真伪,未经简化即可证明它与碎片的上下文有联系。
- 在文件中说明:是的。 文件说的地方:主 741,主 961
- 休息:完整性检查值以理想的MAC为模式,覆盖整个碎片,包括其头状字段; 密钥协议被理想化为共享密钥,加密是没有代数特性的构造器-破坏器对
- 下一步:网络攻击者不需要.

R02:不重放碎片集成员

在单个 IKESA范围内， 同一 (减:ID,碎片数,共计碎片数).的分片至多被接受一次， 重复到达必须被丢弃。

一个与ID,碎片编号和总碎片相同的碎片没有两次被带入队列:重复的碎片被识别并投放,只有一个编号为1的碎片已经处理的请求生成一个答案,即回复的重传. 这是在未滚动到三个片段到达的接收器上确定的,这是任何会议模式不能给出的答案的一半,因为排队是一个会改变的值。

- 结果:在约束范围内持有(变化中的值未滚动为3步); 回答问题:部分; 可用备注
- 值介质:它显示文档的重播规则在接收器真正保持的状态上工作,并注明了绑定值.
- 在文件中说明:是的。 文件说的地方:主 608,主 670
- 休息时间: 固定。 pv 将接收器打开给3个碎片到达者,将发送器打开给2个碎片和1个转发器; 队列持有所储存碎片的设定身份; 文档不固定其数据结构; 重新组装的超时和任何每排容量都没有模型化
- 打开: 队列超时后发生的事情不是模拟的 ; 没有记录有约束的证据的控件查询
- 下一步:模拟超时和在同一IKESA的第二个请求,以查看是否可以恢复一个呆板的队列条目.

A08:重新组装设定一致性

重组成功时， 所有分片的 Message ID 方向、 Total Flagments 一致， Fragment 编号 覆盖 1. . 共计 且不重复, N 次有效载荷 只在第一片非零； 不同集合的分片不会被混合。

碎片合并成一个消息属于一个集:同一个IKE SA,同一个訊息 ID,相同的Total Flagments,第1号碎片与一个非零的Next Biveload和2号碎片为零,没有碎片编号被摄入两次. 将另一集的碎片混合到接受的信息中不会发生.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:它确认了文档所要求的一套一致性,并注明了两段绑定值。
- 在文件中说明:是的。 文件说的地方:主 606,主 619
- 休息:信息固定为两个片段,因此第1段至Total段的覆盖范围是结构模型化的,而不是一个计数; 接收器按文档的顺序检查字段,但模型会修正这些检查
- 打开: 超过两个片段, 以及一个更大的总片段重新开始重新组装的规则, 不模拟 。
- 下一步:模型三块碎片和重启规则,以覆盖PMTU的发现案例.

K01:IKE SA 密钥和IKE_AUTH 内容密钥

攻击者不能推导出 SK_ei、SK_er、SK_ai、SK_ar 以及由它们保护的 IKE_AUTH 内容。

两个方向的加密和完整性密钥和破碎的IKE_AUTH的受保护内容都无法由网络上的攻击者获得,尽管同一消息中携带的发起者身份是公开的. 攻击者看到每一个碎片,它的初始化矢量及其完整性检查值,并且从中什么也学不到.

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:这是从IKE SA中继承的、为零散信息所证明的保密性; 警告是理想的关键协议。

- 在文件中说明:是的。 文件上说:rfc7296:562
- 休息时间:IKE_SA_INIT的关键协议被长期共享的秘密所取代,因此前向保密和协议的力度不进行评估; 加密是破坏结构的一对 完整性检查是理想的MAC
- 下一步:一个在Tamarin+ Agent的Diffie-Hellman模型会随着协议的产生而解决密钥的保密问题.

K04:每个方向分别按键

发起方方向与响应方方向使用的加密与完整性密钥不同， 不同 IKE SA 会话的密钥也不同。

1个IKE SA的双向没有共享关键词,2个IKE SAs的密钥因每个密钥来源于新鲜的非ce而不同. 模型显示的是结构后果:一个被接受的片段或答案只在它自己的方向的密钥下被检查过,所以一个方向所保护的值在另一个方向不被接受.

- 结果:持有; 回答问题:部分; 可用备注
- 价值低:这是模型产生密钥的方式造成的; 它证实该模型没有混合方向,但它没有测试从其他角度获取密钥的实施。
- 在文件中说明:是的。 文件上说:rfc7296:568
- 休息:衍生是适用于共享密钥、两个非密钥和方向标签的密钥衍生函数; 这就是模型如何分离方向,文档只要求分离; 读取一个为两个方向服务的密钥可视为双向注册的一个词
- 开放:方向以外的密钥衍生细节和会话标签没有建模; 没有记录控制查询
- 下一步:无; 地产是一个结构性的衍生物。

S01: 单键下无IV再利用

在同一真实密钥下， 每次加密调用使用的完整 00nonce(IV)不重复， 包括重传不视为新加密。 (中文(简体)).

每个片段在会话密钥下用自己的初始化矢量进行加密,再发送一个相同的受保护片段而不是再次加密,因此在一个密钥下没有两个加密共享一个矢量. 这为两个加密和重传模型解卷提供了支撑,即一个不高级的计数器会显示的地方.

- 结果:在约束范围内持有(变化中的值未滚动为3步); 回答问题:部分; 可用备注
- 数值低:它重申了未滚动步骤对矢量的要求; 反语义是执行的,不在文件中。
- 在文件中说明:是的。 文件说的地方: 521号主机
- 休息:发件人未卷入两个片段,再传送一个带界. pv; (中文(简体)). 矢量是一个新值,每加密一次, 代表一个执行保存的计数器; 文件没有具体说明矢量是如何生成的,只是有效载荷携带一个
- 打开:矢量是如何生成的,以及它是否在重键中存活下来,并不是模拟的; 没有记录有约束的证据的控件查询
- 下一步:规格无; 一个执行问题。

S02: 重播处理不回滚状态

重传或重复分片的处理不会回退已安装密钥、清空接收窗口或恢复旧权限； 仅 破碎编号:为 1 的重传可触发响应重传。

处理重复发送或再发送的碎片不会将接收器翻回:请求被处理完毕,队列没有被清除,也没有两次安装消息,已经处理的请求中编号为1的碎片只产生存储答案的再发送. 测试失败的碎片会被丢弃而不触及队列.

- 结果:在约束范围内持有(变化中的值未滚动为3步); 回答问题:是的; 可用备注
- 值介质:它显示重传规则不会撤销状态,这是文档规则背后的担忧.
- 在文件中说明:是的。 文件说的地方: 669号主机

- 休息时间: 固定。 pv 将接收器打开给3名到达者; 清除队列的超时未建模; 答案被缓存为接收器所保存的值,这就是文档在提到重发送响应时所假设的.
- 打开: 没有记录有限制的证明的控件查询
- 下一步: 模拟超时, 以查看过期能否清除仍在填充的队列 。

U01:不将碎片搅拌到各套设备之间

不存在接收方接受重组 IKE_AUTH 而其分片来自不同 新闻 ID 或不同方向的轨迹。

不同信息ID的碎片、其他方向的碎片或另一个总碎片的碎片没有合并成一个被接受的IKE_AUTH:两个被接受的信息的碎片都是在该信息ID下按该方向发出的,并带有相同的总碎片。 每个碎片都在其方向的完整密钥下检查,一个碎片携带的字段都在检查之下。

- 结果:持有; 回答问题:是的; 可用
- 值高:它回答了用户直接问的问题,被证明没有触及绑定的简化.
- 在文件中说明:是的。 文件说的地方: 619号主机
- 休息:方向检查在模型中,如文件头处理中; a. 仅凭每个方向键而省略其内容的接收器,而模型无法将其区分开来; 每IKE SA个破碎的讯息,所以没有执行同一IKE SA的第二次请求。
- 打开:文档打开的个案是接收方的重播测试没有指定方向,该方向作为发现报告
- 下一步:模型无; 规格文本可以指定重播测试中的方向。

U02:在完成重新组装前不接受

不存在接收方在未完成全部分片校验前接受 IKE_AUTH 的轨迹。

接收器只有在收到、检查和合并所有碎片后,才使用IKE_AUTH美元,而电文中则从未使用过。 这就是文件所要求的保护,因为它警告说,仍在飞行中的碎片可以改变已经解析的碎片的含义。

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:它确认文档给出的警告是符合它所表述的规则的,并注明了两段的绑定值.
- 在文件中说明:是的。 文件说的地方: 788号主机
- 休息:重新组装的步骤是模型中的一个明确步骤,在解析之前; 文件除了需要全套文件外,没有调整内部顺序; 绑定两块块
- 下一步:不需要。

U03: AUTH 验收前核实.

不存在接收方在未通过原始 IKE_AUTH 身份验证的情况下接受重组消息的轨迹。

被接受的IKE_AUTH重新组装,总是带有声称身份的签名,上面写着这个交换站的两个非ces和那个身份,答复者在对信息采取行动之前进行验证. 不持有签名密钥的攻击者无法获得被接受的信息以获得身份,因为新鲜的交换有新鲜的非ces.

- 结果:持有; 回答问题:是的; 可用
- 价值高:是交换存在的认证保证,为重新组装的电文和不装订的文档调用的关键所证明。
- 在文件中说明:是的。 文件上说:draft-ietf-ipsecme-ikev2-pqc-auth:618,rfc7296:579
- 休息:签名的八角形缩小为两个非色体和身份; 更多的文件标志,其余文件由IKE SA的完整密钥保护; 签名是理想的, 没有消息代数属性
- 下一步:网络攻击者不需要.

X01:对发起人的响应者认证

发起人只有在答复者将答复真正寄出于同一非记录和身份时,才接受IKE_AUTH份答复; 网络上的任何攻击者都不可能得到IKE_AUTH的响应,没有这样的运行。

发起者只有在响应者运行时才完成IKE_AUTH,且该响应者在响应者下保护了这个IKE SA的发起键,因此交换的双方向都验证了它们的对等点. 反演失败了,因为它必须:一个被回答的响应者可以被阻止到达发起者,所以两个事件不是一回事.

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:它提供所起草的目标所遗漏的相互认证的一半; 警告是理想的关键协议。
- 在文件中说明:是的。 文件上说:rfc7296:272
- 中止:协议涉及非ces和应答者身份; 答复中的SA个数据由完整性密钥保护,但不能单独模拟; 关键协议被理想化为共同的秘密
- 下一步:无; 适用与A03相同的关键协议说明。

附录 C：主张和证明器的答案

证明器对每个目标的记录:所达到的关卡,到达它的查询,是否检查了控制,以及攻击与分析师对每个目标的判决.

目标	级别	界	查询	对照	攻击	主张
A03	proved		a03	检查		证明:1
A04	proved		a04	2中的1人		证明1,1
D01	proved		d01	检查		证明:1
R02	bounded	未滚动到 3 步的数值变化	铜			1 定界,2 可到达
A08	proved		a08_first	3中的2人		证明2,1
K01	proved		k01_key	2中的1人		证明:2
K04	proved		k04			证明:1
S01	bounded	未滚动到 3 步的数值变化	页:1			1 定界,1 可到达
S02	bounded	未滚动到 3 步的数值变化	铜			1 定界,2 可到达
U01	proved		a08_second	检查		证明:1
U02	proved		u02	检查		证明:1
U03	proved		u03	检查		证明:1
X01	proved		x01	检查		证明:1

以分析师对每项主张的措辞提出的主张; 每一个答案都是证明器的:

目标	主张	攻击者	回答	查询	对照
A03	每一次接受重新组装的IKE_AUTH,就相当于IKE SA的真正的发起人运行,其信息相同ID,发起者身份相同,请求的响应者身份相同,谈判数据相同SA,以及两个非编号相同; 攻击者只有网络	network	proved	a03	检查
A04	重复播放或再次转发的已接受请求的片段,不会导致接收者再次接受该请求,因为接收者没有登记到三名抵达者。	network	定界(变化中的数值未滚动为 3 步)	铜	无
A04	每一次接受重新组装的IKE_AUTH次,都有不同的发起人运行:一次运行不能被接受两次,模式是每IKE SA次零碎请求; 攻击者只有网络	network	proved	a04	检查
D01	接收器接收的任何碎片,包括接受的ID号电文、碎片编号、总数和IKE SA,都是由IKE SA号电文的发起人发出的,其内容不变; 在正确的方向密钥下,没有到达其ICV的接收器; 攻击者只有网络	network	proved	d01	检查
R02	片段被带入重新组装的队列:目标所说的情况可以达到.	network	reachable	reach_fragacc	
R02	已经放入重装队列的碎片被确认为重播,并投在未卷到3个碎片到达的接收器上。	network	reachable	空投点	
R02	在一个IKE SA中,一个装有相同信息ID的片段,碎片编号和总碎片,从未被两次收录,此时接收者保持其排队状态,并在每次到达时对其进行比较,未卷到三个到达者.	network	定界(变化中的数值未滚动为 3 步)	铜	无

目标	主张	攻击者	回答	查询	对照
A08	一个集的片段编号没有两次被带入重新组装的队列,因此片段合并成一个信息封面,封面编号为1至Total,没有重复,在接收器上未滚动到三个到达.	network	定界(变化中的数值未滚动为 3 步)	铜	无
A08	重新组装的首个片段, 带有碎片编号1和非零 下一个有效载荷, 在同一信件下发送ID成员名单IKESA作为重新组装的消息; 攻击者只有网络	network	proved	a08_first	检查
A08	重新组装的电文的第二片段是在同一个ID信件下发送的,与第一个一样的全片段,它的下一个有效载荷场为零,因此另一片段的片段没有被合并到它中; 攻击者只有网络	network	proved	a08_second	检查
K01	攻击者可取得IKE SA的任何方向的SK_e或SK_a; 攻击者只有网络	network	proved	k01_key	无
K01	分散的IKE_AUTH请求的保护内容没有到达攻击者手中,尽管同一信息中携带的身份是公开的; 攻击者只有网络	network	proved	k01_content	检查
K04	一个IKE SA的关键词没有为两个方向服务:响应键的发起者与发起键的响应者是不同的,不同IKE SAs的密钥是不同的,因为它们来自新鲜的无色; 攻击者只有网络	network	proved	k04	无
S01	发送并接受用自己的IV来保护的碎片:目标所说的情况是可以达到的。	network	reachable	reach_fragacc	
S01	对会话密钥下的一个片段的每一个加密都会使用它自己的初始化矢量,而第一个片段的重传会重新发送相同的受保护消息而不再次加密; 发件人未滚动为两个加密和一个再发送。	network	定界(变化中的数值未滚动为 3 步)	页:1	无
S02	片段被拿走,请求得到答复:目标所说的情况是可以达到的。	network	reachable	reach_fragacc	
S02	已处理的请求的第一稿被重新传送,触发了对未滚动接收器的重新传送。	network	reachable	布莱特克斯语Name	
S02	重复发送或再发送的碎片既不会再次安装信息,也不会再次接受:最多一次接收同样的碎片身份,处理的请求继续处理,超过三次抵达。	network	定界(变化中的数值未滚动为 3 步)	铜	无
U01	没有其它信件的片段ID或另一个方向的总裂缝合并成一个接受的IKE_AUTH: 重新组装的信件的两个片段都是在本信件下发送的ID,朝这个方向,具有相同的总裂痕; 攻击者只有网络	network	proved	a08_second	检查
U02	在接收、核实和重新组装完整的碎片之前,接受IKE_AUTH号; 攻击者只有网络	network	proved	u02	检查
U03	接受重新组装的IKE_AUTH意味着声称的身份对该交易所的两个非编号和该身份签名; 答复者在对消息采取行动之前先检查一下; 攻击者只有网络	network	proved	u03	检查
X01	发起人只有在应答者在本次交换的非ces和身份上签字后才能完成IKE_AUTH,而该应答则在IKE SA的发起人密钥的应答者下受到保护; 2. 攻击者只有网络	network	proved	x01	检查

附录 D：分析是怎么跑的

LLM名分析员从文件中建立了协议模型,将每个财产归入ProVerif; 第3节中的每一个结果都是证明器的答案.

ProVerif+ 代理会话 session-20261114T232852, 2026-11-14. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:53,校对:98 s,壁16 min,耗资0.128 USD.

ProVerif:56 证明运行,54 决定,2 未答,72 s,35 答录.

分析了什么

协议	IKEv2 加密破解 PQ 认证
版本	rfc7383
分析范围	初始 IKE_AUTH使用 PQ签名的大消息，经 RFC7383SKf分成固定两片；建模独立 IV/完整性保护、消息ID、方向、片段编号/总数,完整重组后才解析认证。固定一个消息、最多两片；不包含UDP丢包活性或任意分片数量的无界资源上限。
不在范围内	符号模型不证明算法的计算安全或抗量子安全；攻击轨迹只在明确假设下成立，不直接等同规范漏洞。每个性质必须有可达性/正例控制。
原文	以下各节的438个编号段落(146139字节). 本报告中的s0001等参考文献就是其中一段。

文件各节的分析依据如下:

文稿	章节	标题
主体	2	协议细节
主体	2.1	概览
主体	2.2	限制
主体	2.3	谈判
主体	2.4	使用 IKE 碎片化
主体	2.5	破碎信件
主体	2.5.1	选择碎片大小
主体	2.5.2	PMTU 发现
主体	2.5.3	包含无保护的有效载荷的零碎信件
主体	2.6	接收 IKE 碎块信件
主体	2.6.1	重播检测和再发送
主体	3	与其他 IKE 扩展的相互作用
rfc7296	2	IKE 礼宾细节和变动
rfc7296	2.1	使用再传送计时器
rfc7296	2.2	信件使用序列号 ID
rfc7296	2.3	重叠请求的窗口大小
rfc7296	2.4	状态同步和连接超时
rfc7296	2.5	版本编号和转发兼容性
rfc7296	2.6	IKE SA SPIs和饼干

文稿	章节	标题
rfc7296	2.6.1	COOKIE和INVALID_KE_PAYLOAD的相互作用
rfc7296	2.7	密码算法谈判
rfc7296	2.8	重键
rfc7296	2.8.1	同时期儿童 SA 重新键入
rfc7296	2.8.2	同时 IKE SA 重键
rfc7296	2.8.3	重修IKE SA对重修
rfc7296	2.9	交通选择谈判
rfc7296	2.9.1	交通选择者侵犯自有政策
rfc7296	2.9.2	Rekeying 中的交通选择器
rfc7296	2.10	诺斯
rfc7296	2.11	地址和端口敏捷度
rfc7296	2.12	Diffie-Hellman 指示器的重新使用
rfc7296	2.13	生成密钥材料
rfc7296	2.14	生成IKE SA型机车的密钥材料
rfc7296	2.15	IKE SA号机车的认证
rfc7296	2.16	广泛认证协议方法
rfc7296	2.17	制作儿童密钥材料 SAs
rfc7296	2.18	重键IKESAs使用aCREATE_CHILD_SA交换
rfc7296	2.19	请求远程网络内部地址
rfc7296	2.20	请求对等版本
rfc7296	2.21	处理错误
rfc7296	2.21.1	IKE_SA_INIT中处理错误
rfc7296	2.21.2	IKE_AUTH中处理错误
rfc7296	2.21.3	IKE SA 后处理错误已认证
rfc7296	2.21.4	处理错误 IKE SA
rfc7296	2.22	IPComp
rfc7296	2.23	NAT 倾斜
rfc7296	2.23.1	运输方式 NAT Traversal
rfc7296	2.24	明确通知(ECN)
rfc7296	2.25	交换碰撞
rfc7296	2.25.1	恢复或关闭时的碰撞 SAs
rfc7296	2.25.2	收回或关闭时碰撞 IKE SAs

协议的目的是在文档中将其定位为源步骤:初始 IKE_AUTH使用 PQ签名的大消息，经 RFC7383SKf分成固定两片；建模独立 IV/完整性保护、消息ID、方向、片段编号/总数,完整重组后才解析认证。固定一个消息、最多两片；不包含 UDP丢包活性或任意分片数量的无界资源上限。

对照文稿定性质

在写出查询之前,分析师根据文件本身所说的协议的目的设定了已起草的属性清单. 名称、财产是什么 以及文件上所说的 是分析师的读物; 文档中存在指定位置。

ID	简称	对象	文稿怎么说	出处
A03	重新组装后的IKE_AUTH协议	IKE_AUTH交换机中的应答器:该交换机的发起人身份和AUTH有效载荷,以及谈判的SA数据,可以保证它何时接受重新组装的请求.	重新组装的碎片被合并到原始信件中,然后作为常规处理IKE消息(简讯)s0081),以及AUTH有效载荷证明知道该秘密与IDi以信件和对等者的非曲直表示(s0271;rfc7296:585).	rfc7296:585, s0003, s0081
A04	每个启动程序接受一次	响应者:最多接受一次发起者IKE_AUTH的单次运行; 同一片段集的再传输和重播并不能给出第二次接受.	电文的转发MUST使用相同的信件ID(rfc7296:108),与信件一起使用碎块编号和全部碎块ID检测再传播和重播(s0086,s0087),并带有碎片编号的重复碎片。1必须忽略(E)s0088).	rfc7296:108, s0077, s0086, s0087, s0088
D01	单个碎片的真实性和约束性	IKE条断块电文的接收者:解密的内容及其上下文,ID条电文,方向,断块编号和总断块,是被允许发送的发件人; 3. 没有改变碎片,也没有储存或使用任何碎片使其ICV失效。	在加密和认证之前就发生了碎片化,使每个碎片都得到单独的保护,使接收器可以丢弃伪造的碎片而不是储存这些碎片(s0003、s0030); ICV号经过核实,在故障时,电文被悄悄地丢弃(s0078); IKE号机头在除长度和下一个有效载荷(s0040)外的每个碎片中均完好无损地行驶.	主机:741,主机:961,s0003,s0030,s0040,s0078
R02	不重播一个碎片集成员	IKE SA号的重装队列:一个片段与同名的訊息ID号,已排入队列的碎片编号和总碎片是重播,不得再收录.	如果一个带有相同信件的片段ID,断块数和总断块数已经在重组队列中 。MUST被默不作声地抛弃(s0077); 相同领域MUST随信件一起使用ID检测重播(E)s0087).	主机:608、s0077、s0087
A08	重新组合设定一致性	重新组装IKESA号的队列:碎片合并成一个原始消息,都属于同一套,同一套消息ID号,方向和总碎片相同,覆盖了编号为1的碎片至Total,没有重复,只有第一个碎片搭载了非零的下一个有效载荷.	碎片数量必须是非零的,且不大于总碎片,而总碎片数量必须是非零的(s0037,s0038); a. 储存的装置不得与另一套总碎片(s0075、s0079)混合; 第一个碎片的下一个有效载荷是第一个内载荷,其余的为零(s0036); 总裂缝区分了不同阈值(s0059,s0060)生产的套件.	主机:606,s0036,s0037,s0038,s0059,s0060,s0075,s0079
K01	IKE SA 密钥和 IKE_AUTH 内容密钥	两个同龄人:每个方向的SK_e和SK_a,以及他们保护的IKE_AUTH有效载荷内容,都从网络攻击器中保留下来.	SK_e及SK_a(rfc7296:560-573)对IKE_SA_INIT00之后的电文进行加密并保护完整性,在原始电文加密和认证之前进行破碎,因此碎片内容的保护方式相同(s0003,s0030,s0033).	rfc7296:562, s0003, s0005, s0030, s0033
K04	每个方向分别按键	两个对等点: 发起方对响应方方向的加密和完整性密钥不是响应方对响应方方向的密钥,一个IKE SA的密钥不是另一个IKE SA的密钥.	每个方向(rfc7296:568)分别计算出一个SK_e和SK_a,每个IKE的电文,包括信头在内,都是以该方向的SK_e和SK_a(rfc7296:564-573)保护完整性的.	rfc7296:568, s0030, s0031
S01	单键下无IV再利用	IKE断裂消息的发送者:在SK_e下对片段的每一个加密都使用新的初始化矢量,再传输的片段是相同的受保护消息,而不是新的加密.	加密碎片有效载荷携带自己的初始化矢量,其加密处理是加密有效载荷(s0030,s0034); 重传保存了ID号电文,因此保存了受保护电文(rfc7296:108,s0088).	主机:521、s0030、s0034

ID	简称	对象	文稿怎么说	出处
S02	重播处理不向后滚动状态	接收器:处理重复的或再传送的碎片,既不再次安装密钥,也不清理重新组装的队列,也不恢复旧的接受; 只有一个碎片 编号1 触发重传答案。	重复的碎片必须静悄悄地丢弃(s0077),已经处理的请求的重传碎片只能触发反应的重传,而且只有在其碎片编号为1(s0088)时才触发.	主机:669、s0077、s0088
U01	不将片段搅拌到各组之间	IKE SA号的复编队列:不同消息ID号的片段,另一方向的片段,或另一条总断层的片段,从未合并成一个接受的IKE_AUTH号片段.	接收器必须检查接收到的碎片总碎片是否与已储存的集相匹配,并在生长时重新开始重新组装(s0075,s0079),合并内容作为IKE常规电文(s0081)处理; 用户明确询问此信息以获取 ID 消息和方向。	主机:619、s0060、s0075、s0079、s0081
U02	完全重新组装前不接受	一个破碎的IKE_AUTH的接收器:它只在接收、核实和合并所有破碎后,才对消息进行剖析和操作,从没有在已有的起点上。	当收到所有碎片时,解密内容作为常规信息(s0081)进行合并和处理,文件警告说,在重新组装之前对已有的有效载荷采取行动是完整的,攻击者可以加以利用(主要为:780-790)。	主机:788、s0080、s0081
U03	接受前核实的AUTH	回应者:只有在AUTH有效载荷通过声称的身份的密钥验证后,它才接受重新组装的IKE_AUTH,并且该消息否则会被丢弃.	合并的电文作为IKE条普通电文(s0081)进行校验和解密; 3. 双方签署对方的非ce,这样做对交易所的安全至关重要(s0271); 每个会话的签名数据是独一无二的,因为非会话(draft-ietf-ipsecme-ikev2-pqc-auth:618)。	draft-ietf-ipsecme-ikev2-pqc-auth:618, rfc7296:579, s0081, s0271
X01	响应者对发起人的认证	发起人:通过核实应答人AUTH的有效载荷,在完成IKE_AUTH交换时,可以保证应答人的身份和谈判数据。	IKE进行双方相互认证(rfc7296:272); 第二对电文认证了以前的电文和身份(rfc7296:483-489); 答复者在发起人的非ce上签注,发起人在答复人(s0271)上签注. 起草的目标只谈到重新组装请求的接收者,因此发起者一方没有被覆盖.	rfc7296:272, rfc7296:483, rfc7296:585, s0271

分析者依据文稿补充的性质：X01.

文稿里的安全表述，逐段去向

宿主把文稿里说明协议保护什么、防什么的章节逐段列出，共 50 段；分析者对每一段说明了去向：定为性质、定为攻击者条件，或者为什么都不选。选了 5 段，没选 45 段。列哪些段落由标准的章节结构决定；每一段的去向是分析者的判断。

段落	出处	定为	不选的原因
P01	draft-ietf-ipsecme-ikev2-pqc-auth:595-610	A03, D01	
P02	draft-ietf-ipsecme-ikev2-pqc-auth:612-620	A03, U03	
P03 至 P08	draft-ietf-ipsecme-ikev2-pqc-auth:622-662	证明器问不了	PQC签名计划的安全级别,它们与NIST类和2^64签名限制SLH-DSA的安全级别比较: 原始人的强度和使用限制,不能问象征性的证明器.
P09	主机: 739-744	D01	

段落	出处	定为	不选的原因
P10 至 P12	主机: 746-770	证明器问不了	避免了IP的破碎,一个完成IKE_SA_INIT的攻击者在所述的攻击中发送了一大堆但不完整的碎片来耗尽接收器的重新组装记忆,以及建议的队列尺寸限制:一个资源耗尽和储存的碎片数量,一个象征性的证明器是不能问的. 任务边界排除了未限定的资源限制,攻击中的攻击者持有自己IKE SA的密钥,而这个模式来源于它无法计算的一个共同的秘密.
P13	主机: 772-778	没有陈述目标	关于选择重新组装队列大小及其配置的建议; 它规定不得持有或攻击任何财产。
P14	主机: 780-790	U02, network	
P15	rfc7296:6478-6488	不在范围内	它描述了在IKE_AUTH被认证之前,未经认证或反应者模仿的同伴可以了解发起人的身份和证书。 IKE_SA_INIT的关键协议在此型号之外(IKE SA密钥来源于一个长期共享的密钥),因此探测攻击者无法模拟; 记录为限制。
P16	rfc7296:6490-6494	不在范围内	约EAP次认证,任务未涉及; 2. 签名认证是模拟的。
P17	rfc7296:6496-6500	不在范围内	与CREATE_CHILD_SA重键; 仅模拟了IKE_AUTH次交流。
P18 至 P20	rfc7296:6502-6527	证明器问不了	Diffie-Hellman集团和谈判原始人的力量:一个原始人的力量,一个象征性的证明器是不能问的; IKE_SA_INIT关键协议也在模型之外.
P21	rfc7296:6529-6530	证明器问不了	Diffie-Hellman的代言人被假定从记忆中抹去:一个与记忆相关的执行属性,而不是协议的属性.
P22	rfc7296:6532-6538	证明器问不了	执行工作必须强有力地对付未经认证的同行和DoS次袭击,特别是在EAP:可用性和执行工作的有力性,不能要求象征性地证明这一点。
P23 至 P24	rfc7296:6540-6549	证明器问不了	PRF型的输出大小和随机性的质量:一个原始的强度和随机数生成器的属性.
P25	rfc7296:6551-6556	不在范围内	关于谈判NONE完整性保护或ENCR_NULL的禁令:算法谈判不属于这个模式,它确定了IKE SA号的保护.
P26	rfc7296:6558-6563	不在范围内	来自密码的预共享密钥会受到字典和社会工程攻击. 该模型只使用一个长期共享的秘密作为IKE_SA_INIT关键协议的理想化站点,所以真实的PSK的可猜性并不是本协议的模拟财产; 记录为限制。
P27 至 P28	rfc7296:6565-6580	不在范围内	大约NAT份检测通知和它们可能泄露的内部地址; NAT transversal位于模型之外.
P29 至 P30	rfc7296:6582-6612	不在范围内	约EAP方法,在EAP之前不会生成一个密钥和服务器的公钥认证; 3. EAP位于模型之外.
P31	rfc7296:6614-6619	证明器问不了	IP重装缓冲器的耗尽,IKE破碎的用意是避免:资源耗尽不能询问证明器,任务边界排除.
P32	rfc7296:6621-6625	不在范围内	接收控制、信任锚和部署的安全政策; 这些是协议交换模式外的配置选择。
P33	rfc7296:6631-6633	证明器问不了	执行的脆弱性和无限制的EAP条信息:执行的有力性和可用性,不能问其具有象征意义的证明。
P34 至 P41	rfc7296:6637-6696	不在范围内	同行授权数据库和流量选择器授权; 该模型没有交通选择器有效载荷,也没有政策数据库,任务是破碎IKE_AUTH。
P42 至 P45	rfc7427:398-420	证明器问不了	推荐的散列函数,将签名,散列和曲线的安全级别混合在一起,以及由此产生的最弱部分的弱点:原始人的强度,不能问一个象征性的证明器.
P46	rfc7427:426-429	A03, U03	

段落	出处	定为	不选的原因
P47 至 P50	rfc7427:431-449	证明器问不了	降级为灾难性的弱密码,排除了MD5,已知的弱点RSASSA-PKCS1-v1_5和SHA-1:原始人的强项,一个象征性的证明器是不能问的.

参与方和受保护的值，逐项是否设为攻击者条件

宿主把起草的性质里点到的参与方和受保护的值逐项列出，共 27 项；分析者对每一项说明了哪个攻击者条件控制这个参与方或持有这个值，或者为什么不设。设了攻击者条件的 0 项，没设的 27 项。清单来自性质本身；每一项怎么处理是分析者的判断。

ID	参与方或值	类别	攻击者条件	不设的原因
S01	发起方	参与方	攻击者得不到更多	一个不诚实的发起者担任发起者的角色:它只能发送一个它真正产生的碎片,这是D01和A03所要求的,它没有掌握反应者方向的关键.
S02	响应方	参与方	攻击者得不到更多	一个不诚实的回答者只能拒绝或回答它真正参与的操作; 它不掌握发起者方向的密钥,所以它不会学习网络攻击者缺乏的关于发起者请求的东西.
S03	攻击者	参与方	攻击者得不到更多	S03是攻击者本身; 只有网络的攻击者是每个目标都得到答复的基线攻击者,所以它除了它之外没有增加任何东西。
S04	IKE_AUTH 中的身份与认证数据	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S05	协商的 SA 参数	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S06	电文 ID	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S07	断裂数	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S08	残块共计	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。

ID	参与方或值	类别	攻击者条件	不设的原因
S09	重组后的 IKE_AUTH	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S10	SKF 载荷内容	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S11	ICV	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S12	分片标识三元组	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S13	重组队列	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S14	下一个有效载荷	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S15	方向标志	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。

ID	参与方或值	类别	攻击者条件	不设的原因
S16	SK_ei	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S17	SK_er	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S18	SK_ai	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S19	SK_ar	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S20	IKE_AUTH 明文内容	值	按定义全部失守	这些是身份AUTH财务报告和财务报告SA重新组装的数据IKE_AUTH, 其密码和简写, 在每个片段中行走的页眉字段(Message)ID, 碎片编号, 总碎片, 下一个有效载荷, 方向旗,ICV,IV),两者SK_e和两个SK_a,和重新组装的信息。 拥有信头字段和IV是网络攻击者已经拥有的东西; 保存内容或密钥IKESA所以这里要求的每个财产 都从定义上说都丢失了 这些文件不要求提供保护,主要是:752有攻击者计算SK_a财务报告和财务报告SK_e其国家IKESA这是资源攻击,不是保密要求。
S21	初始化矢量	值	按定义全部失守	重新组装的队列及其状态,安装的密钥,响应缓存,碎片内容,AUTH有效载荷和身份:谁控制它们就具有接收器状态,因此此处要求的重新播放,重新组装和协议属性被定义为丢失,文件要求不受持有它们的一方的保护.
S22	已安装密钥	值	按定义全部失守	重新组装的队列及其状态,安装的密钥,响应缓存,碎片内容,AUTH有效载荷和身份:谁控制它们就具有接收器状态,因此此处要求的重新播放,重新组装和协议属性被定义为丢失,文件要求不受持有它们的一方的保护.
S23	重组队列状态	值	按定义全部失守	重新组装的队列及其状态,安装的密钥,响应缓存,碎片内容,AUTH有效载荷和身份:谁控制它们就具有接收器状态,因此此处要求的重新播放,重新组装和协议属性被定义为丢失,文件要求不受持有它们的一方的保护.
S24	响应缓存	值	按定义全部失守	重新组装的队列及其状态,安装的密钥,响应缓存,碎片内容,AUTH有效载荷和身份:谁控制它们就具有接收器状态,因此此处要求的重新播放,重新组装和协议属性被定义为丢失,文件要求不受持有它们的一方的保护.

ID	参与方或值	类别	攻击者条件	不设的原因
S25	分片内容	值	按定义全部失守	重新组装的队列及其状态,安装的密钥,响应缓存,碎片内容,AUTH有效载荷和身份:谁控制它们就具有接收器状态,因此此处要求的重新播放,重新组装和协议属性被定义为丢失,文件要求不受持有它们的一方的保护.
S26	AUTH 载荷	值	按定义全部失守	重新组装的队列及其状态,安装的密钥,响应缓存,碎片内容,AUTH有效载荷和身份:谁控制它们就具有接收器状态,因此此处要求的重新播放,重新组装和协议属性被定义为丢失,文件要求不受持有它们的一方的保护.
S27	身份	值	按定义全部失守	重新组装的队列及其状态,安装的密钥,响应缓存,碎片内容,AUTH有效载荷和身份:谁控制它们就具有接收器状态,因此此处要求的重新播放,重新组装和协议属性被定义为丢失,文件要求不受持有它们的一方的保护.

每条性质在各攻击者条件下的答案

攻击者是分析师的,在写出询问之前设定的; 每一个答案都记录在其中之一下。 牢房是攻击者的财产的证明器答案; "无答"是攻击者设定的,用于证明器未裁定索偿或无记录的财产; 2. 空单元格是分析师没有为财产设定的攻击者。

攻击者	持有什么	依据	出处
network	只有网络:它读、丢、更改和发送消息,并且不为一方保密		

ID	network
A03	成立
A04	成立
D01	成立
R02	成立
A08	成立
K01	成立
K04	成立
S01	成立
S02	成立
U01	成立
U02	成立
U03	成立
X01	成立

关于证明和模型的说明

- A04:在ProVerif中回答,分析师的名字是changing_state。
- R02:在ProVerif中回答,分析师的名字是changing_state。
- A08:在ProVerif中回答,分析师的名字是changing_state。
- S01:在ProVerif中回答,分析师的名字是changing_state。
- S02:在ProVerif中回答,分析师的名字是changing_state。

- U02:在ProVerif中回答,分析师的名字是changing_state。

一个简化代数的ProVerif型号(xor,dh_algebra,other_algebra)给予攻击者少于实际操作:一个证明有针对较弱攻击者的证据,一个攻击有攻击. 一个ProVerif模式,不检查一个值变化(changing_state),让各方接受更多的:一个证据存在,攻击可能只有缺失的支票. Tamarin + 代理型号是这些。

一步步的束缚就是一个有限度的答案。 pv:分析师的第二个ProVerif型号,其中保持变化的值的一方在其支票到位后,不会卷到那许多步骤上. 这个模型比协议做的要少 所以这些步骤的地产 不再继续了 发现有攻击 步骤数是分析师的语句.

分析师的国家审查

这一部分是分析师自己对来源的解读,而不是证明器的答案. ProVerif所示的"是"意味着ProVerif在未滚动模型中发现了带有这些步骤的痕迹,所以这些步骤是可能的; 他们破解目标 只能通过攻击 答案表, 和他们的成本是分析师的阅读。 "什么也没有发现" 说哪些模式被看 并证明什么。

值	保存于	何时更改	检查时间	参考文件
重新组装队列条目: 存储的碎片及其解密内容的设定身份(Message ID, Flagment number, Total Flagments)	回复对等方(接收破碎的IKE_AUTH)	a. 碎片通过碎片编号测试和ICV检查并储存(s0080); 当一个较大碎片的碎片到达时,整个队列被丢弃,并用该碎片重新组装(s0079); 当集完成后,内容被合并,队列条目被删除(s0081); 所有交换的碎片均予丢弃(s0082美元)	每个到达的碎片,在储存任何物品之前:非零碎片数和总碎片数,总碎片数不大于总碎片数,总碎片数不小于所储存的成套碎片数,没有输入相同的信息ID、碎片数和总碎片数(s0072-s0077、s0087)	s0072, s0073, s0074, s0075, s0076, s0077, s0079, s0080, s0081, s0082, s0087
已处理的请求状态和已处理请求的缓存答复	响应端点	整套软件进行了重新组装、核查和处理,并发送了答复(s0081、s0088)	在重复的片段上,决定是否重新发送答案:只有一块有1号碎片触发它,否则片段被忽略(s0088)	s0081, s0088
信息ID 计数器:下一个信息ID用于本方的请求,以及预期同行的下一个请求	双同龄人,每IKE SA个对数	发出请求或收到请求; 答复载有请求的ID号信件,不推进柜台(rfc7296 2.2)	答复与请求相符,接收到的ID号邮件连同碎片编号和全部碎片一起用于重播探测(s0086、s0087)	s0086, s0087, s0088, s0108, s0110

模式	结果	目标	显示于 ProVerif	步骤
重播(E)	没有找到			旧的片段不再被接受:随着队列条目和处理请求状态的保存,同一集的重复片段被丢弃,没有进行第二次接受(绑定). pv,3名抵达者,经核实的回放查询; 滴滴和回答重递是可达到的。
repeat_one_time_action	没有找到			IKE_AUTH号被接受一次; 重复的碎片 1 只能导致重新发送存储的答案,而绝不导致第二次接收或第二次安装电文(捆绑)。 (中文(简体)).
脱同步	没有找到			一个被放弃的零碎请求让请求者重新发送同一份信息ID(rfc7296 2.2),而回复者删除了不完整的请求,并视其为没有到达请求,而不是IKE SA故障(s0082,s0084); 答复者的预期只有经过完全核实的请求(s0081)才能得到推进,所以两个计数器重新步入正轨或IKE SA被删除; 2. 在继续交换时,文档中的任何步骤都无法将它们分开。
update_before_check	没有找到			对一个碎片的ICV检查先于储存(s0076,s0078,然后是s0080):文件丢弃了一个在进入队列前没有经过任何测试的碎片,只有在收到的碎片通过检查(s0079)后才重新开始排队.

模式	结果	目标	显示于 ProVerif	步骤
no_rollback_on_failure	没有找到			一个被拒绝的片段使队列不变(s0076,s0077),一个废弃的交换机删除了不完全的请求,而没有其他任何回滚(s0082,s0084); 已经处理的请求仍待处理,因此,以后的片段无法取消接受。
race_between_sessions	候选人		否:没有以ProVerif进行审判	在一个IKE SA的双向中,可以使用相同的訊息ID值:原发起人的n请求,它的响应,原响应者的n请求及其响应都带有n(rfc7296 2.2). / RFC 7383的重播测试只比较了Message ID,碎片编号和总碎片对队列(s0077). 方向旗不是测试的一部分。 / 所以,一个响应者请求的片段,与同一个消息ID,断块数和总断块将无法单独通过测试与发起者的片段区分开来,一个队列为双向服务. / 分离完全建立在每段ICV和每段方向键上:IKE信头在每一个片段(s0040)中行驶完好,包括信头在内的整条信息是完整保护的(rfc7296 3.14通过s0031),每个方向分别计算一个SK_a(rfc7296 2.14). / 后果:在ICV控股期间没有攻击成功,但书面的重播规则本身不排除其他方向,一个检查最后一个ICV的接收器,或共享一个SK_a的双向,将合并两个队列.
distinguishable_failure	候选人		是: ProVerif 伪造 `bretx` 页:1	未能进行任何数字测试或ICV支票的碎片被默不作声地丢弃(s0076,s0078),因此这些拒绝没有给出答案. / 已经处理过的请求的重复片段以两种不同的方式得到回答: 以1号碎块引发了回复的重传,其他的碎块号则被忽略(s0088). / 因此,提出原始碎片的路面攻击者从重复发送的回复中得知,请求已经处理,从沉默中得知,请求没有处理; 文件中没有任何内容禁止这样做,而且从未看到碎片的一方无法得到答案,因为ICV号武器必须加以核实。
wrap_or_window	没有找到			总碎片场只增加,更大的值抛弃了存储的集合(s0079),碎片号必须位于1和总碎片之间(s0077上下文,s0037,s0038); 由于只有持有SK_a的发送者才能产生一个通过ICV的碎片,任何攻击者都无法移动接收窗口,并且球场以有效载荷的16位编码为界. 重新组装的超时(s0082)是一个定时器,在证明器所问的之外.

分析师给目标取了什么名字?

步骤	目标	特性	原因 :
44	R02, S02, A04, A08, S01, U02	changing_state	这些目标依赖于一个政党所保存的值和变化:与存储的碎片的设定身份(Message ID,Flagment number,Total Flagments)重新组装队列,一个请求已经与缓存的响应一起处理,Message ID计数器,以及初始化矢量计数器. 他们的回答是有限度的。 pv,接收器和发送器被解卷到三个碎片到达的地方,州检涵盖解卷之外的东西.
44	A03, D01, K01, K04, U01, U03, X01	plain_primitives	这些目标仅依赖于密钥衍生、以初始化矢量、完整性检查值和签名进行加密,这些签名都是以失败行为为模式的理想原始人; 除构造器-破坏器方程外,不使用代数定律。

分析员的结语

所有13个目标(12个起草后加上1个附加目标,响应者认证发起者)都对网络上的攻击者有答案. 9个被证明是ProVerif: 碎块真实性和对碎块具有约束力IKESA、 信件ID、方向、碎片数量和总碎片D01),认同身份,SA重新组装后的数据和非数据(A03),每跑一次验收(A04),不将碎片搅拌到各组之间(A08,U01),在完全重新组装之前不接受(U02),AUTH在行动前通过该交换的非交易进行核实(U03),对应方的相互认证(X01和保密性IKESA密钥和受保护的密钥IKE_AUTH内容(A)K01). 重新播放、再传送和初始化矢量主张(R02,S02,S01,然后重播 半个A04联 合 国A08),在定界上回答. pv与接收器未滚动到3个片段到达,发送器为2个片段加1个重传:相同的片段身份从未被两次接收,处理的请求仍被处理,只有存储的答案被重传,没有两种加密共享一个初始化矢量.K04答案只是作为关键衍生物的结构属性。 没有失败:没有发现对破碎的攻击,两个报告的调查结果是文件所记载的漏洞,而不是攻击的漏洞。RFC7383§2.6不指定方向, 尽管一个IKESA使用相同的信件ID对重复的第一块碎片的授权答复告诉一名上行攻击者该请求是否已经处理。 哪些因素阻碍取得更强有力的成果:IKE_SA_INIT被理想化为一个共同的秘密,因为ProVerif不在此信件结构的Diffie-Hellman模型上终止; 信息固定为两个片段; 暂停时间不是模拟的; 而资源耗尽的攻击 文档本身所声明的 是在可以问到的证明器之外。 一个Diffie-Hellman和Tamarin+ Agent的多裂模型可以解决前两个问题.