对AF个推论进行安全分析,这些推论是当地训练有素的示范分支

19.2.0 — ProVerif+ 代理 报告

文稿	5G系统; 应用函数人工智能/机器学习服务(AI/ML); 第3阶段(第协议定义）阶段)
检查的性质	11 条：10 条成立，0 条不成立，1 条没有答案
发现	无

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

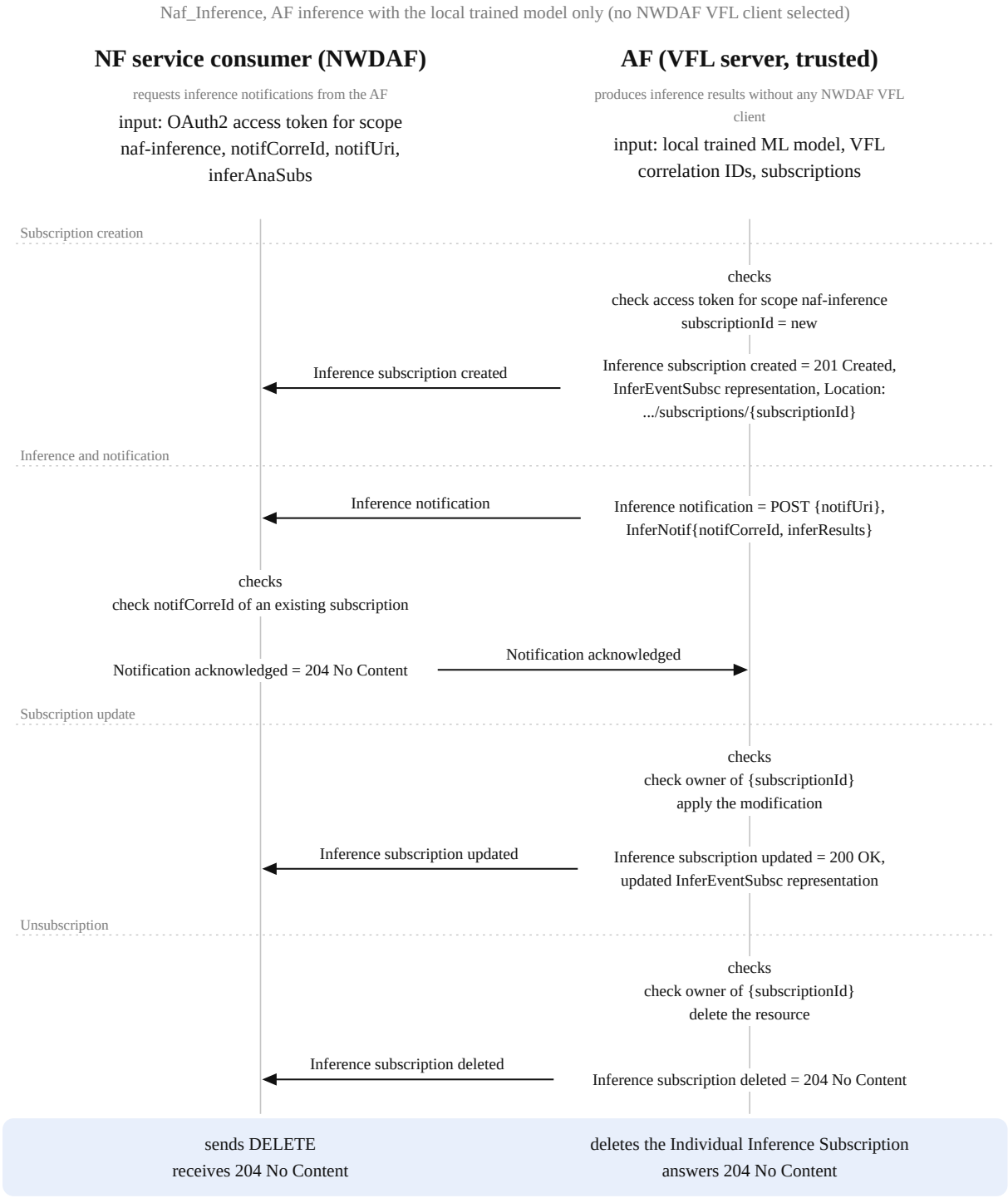
Naf_Inference服务是应用程序函数作为VFL服务器的基于服务接口. 一个NF的服务消费者,这里的NWDAF订阅推论事件通知,可能修改订阅和后来的不订阅,AF报告推论事件回溯到它. 在这个配置中,AF号拥有自己的训练有素的模型,并且选择了没有NWDAF VFL的客户端,因此它报告的结果只来自它的当地训练有素的模型,与它确定的VFL相关. ID.

消费者持有OAuth200的进入证,用于单一服务范围推论、VFL相关联的IDs及其创建的分析订阅; AF拥有经过培训的当地模式和个人推论订阅资源及其notifUri和notifCorreId。 当交换结束时,消费者确信它持有的订阅是它所创建的订阅,并且它所收到的结果是为该订阅而计算的,AF公司确信它所完成的每一个创作,修改或取消都来自拥有订阅并持有有效标志的NF.

双方:

- **NF服务消费者(NWDAF**: 请求缔约方提交推论通知。AF. 持有量 :OAuth2范围参考的存取符号,notifCorreId,notifUri,inferAnaSubs.
- **AF(VFL服务器,可信)**:在没有NWDAF VFL客户端的情况下产生推论结果. Holds:当地训练的ML型号,VFL相关IDs,订阅.

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

没有发现。 分析发现文件没有说明或搁置任何内容。 款次中的表格3对每一个财产都有结果。

没有发现: 在信任范围内 --AF分支Naf_Inference使用当地训练的模型,每个目标都得到回答,没有发现对协议的攻击. 密码AF将每个订阅都与创建它的消费者 和该消费者的存取信号,所以,NF无法创建、修改或取消其它符号NF订阅, 和控制权显示, 没有所有权检查, 它可以。 在未滚动的生命周期中,被删除的订阅既未通知,也未再次修改,每个订阅都有控制。 本地模式的结果按订阅的关联性计算ID并被封存在AF/消费者会话,消费者只接受自己关联的ID和召回终点的通知. 两个答案比证明弱:结果的保密性无法在微量层次解决,更新后结果的新鲜性取决于AF因为InferNotif带不载版本。 分析复制了文件状态的限制,一个整体服务范围API不存在资源级范围,且不记名证券被泄漏后使持有者拥有的无记名证券:NF.

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	**由消费者自己提出要求。** 每当 NF 消费者接受一次订阅创建/更新/取消的成功响应，就存在一个与之匹配的、由该消费者自己发起的订阅请求，且 subscriptionId、notifUri、notifCorreId 与请求中的值一致；每当 AF 发出一次通知，就存在一个此前由该消费者创建或更新、且 notifUri 与 notifCorreId 匹配的订阅。	无	成立	中	否
A08	**与本地模型推论有关的通知。** 每当 AF产生并返回/通知一次本地模型推理结果，该结果所携带的 VFL相关性ID与订阅中确定的 相关性ID一致，且通知发往该订阅的 notifUri并携带该订阅的 notifCorreId。	无	成立	中	否
Z01	**每项行动所需的变异代号。** 每当一个受保护操作（订阅创建、更新、删除，或通知被接受）被提交，提交方持有由 NRF 签发的、对该操作有效的 OAuth2 令牌；无有效令牌的请求不产生受保护副作用。	无	成立	中	是
Z03	**托肯持有人是订阅者。** 每当一个令牌被用于更新或删除某个 subscriptionId 的订阅，该令牌的持有者就是该订阅的创建者（或经授权的实体），且令牌的受众为 AF； 令牌不能被用于其他订阅或其他操作。	无	成立	中	是
Z04	**未签署后无通知。** 每当一个订阅被成功删除（或 AF 以 termCause 终止），此后 AF 不再为该订阅发送新的通知，且针对该 subscriptionId 的更新不再生效。	无	在一个约束内持有(变化中的数值未滚动到4步)	中	否
S05	**未订阅后被拒绝的旧标识符。** 订阅删除生效之后，使用旧 subscriptionId、旧 notifUri 或旧 notifCorreId 的请求不能触发新的通知或修改订阅。	无	在一个约束内持有(变化中的数值未滚动到4步)	低	否
K02	**目标身份和结果来自其他NFs。** 订阅请求与通知中的目标身份（supis,gpsis, intGroupIds, exterGroupIds) 与推理结果只对发起订阅的消费者和 AF 可见，其他 NF 与外部攻击者不能获得。	无	只确认可达	低	不确定
K01	**Token和TLS密钥从攻击者那里保留下来。** 攻击者不能获得 NF 消费者的 OAuth2 访问令牌，也不能获得消费者与 AF 之间 TLS 会话的密钥。	无	成立	低	是
A08.9	**成果带有匹配的订阅和关联标识。** 每当 AF 返回或通知一次本地模型推理结果，该结果所携带的 subscriptionId 与 vflCorrId 与该订阅创建/更新时确定的值一致。	无	成立	中	否
Z03.10	**没有交叉订阅更新或取消。** 一个持有自己合法 OAuth2 令牌的 NF 不能更新或删除另一个 NF 创建的订阅。	无	成立	中	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
U01	**更新后无停滞结果。** 订阅更新生效之后，AF 返回或通知的推理结果不基于更新前的订阅配置；更新前产生的旧结果不能与更新后的配置关联。	无	成立	中	不确定

所问之问,及分析师之答:

问题	回答	依据
Q1:本地结果与订阅 ID,VFL 关联 ID,绑定	模式中的约束性规定:所通知的结果带有它所计算的订阅的关联性数据,消费者的接受与其本身的notifCorreId和notifUri有关; 其中一个漏洞是,通知中未载有subscriptionId号机本身,因此仅消费者就与notifCorreId号机有关。	A08, A08.9, A03
Q2: 合法 NF 跨订阅更新/取消权限边界	号:用自己的有效代币NF号只能作为自己在AF号机上操作,每一次更新或取消都会与持有订阅的车主对照检查,因此另外NF号机的订阅量是无法达到的; 号: 号: 号: 号: 号: 号: 号: 号: 号: 号: 号: 号: 号: 号: 号: 号: 号: 剩下的是无记名证的限制 被泄露的神迹 使持证人达到了NF 这些文件已经说过了	Z01, Z03, Z03.10
Q3: 更新前旧结果与更新后配置的相关性	仅部分:更新后通知的结果与其相关数据的约束,而更新并不改变相关数据,因此消费者无法从更新后提供的结果中得知更新前产生的结果; 来源在InferNotif中定义了没有版本或序列号,而该型号的AF总是重算,所以这取决于AF行为正确,而不是消费者的支票.	U01, A03, A08

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:

- 密码AF被视作信任, 和这个分支,API预设条件; 无人信任的...AF配置通过NEF,通过下列方式间接通信SCP和区域间PLMNSEPP已经超出了范围。
- TLS型是AF型和NF型之间经认证的通道,每个端点有会话键; 该模型无法证明TLS或OAuth2的计算安全性,一个断裂的原始键或漏出的会话键也没有模型化.
- HTTP层(状态代码、错误机构、重定向、特征谈判)没有建模; 拒绝是仿照没有受保护的效果,而不是特定的地位法。
- 订阅标识符是AF产生的新值; 4. 源代码没有说明它们是如何生成的,也没有说明它们是否可以预测。
- 对手案件被脚本化:恶意的NF带着自己的证书发出一套固定的敌对请求,没有程序持有一个泄露的令牌,所以这些行都说支票是做什么的,而不是一个有已知身份识别特征的令牌盗贼能做什么的.
- 订阅生命周期未滚动到四步的界限内. pv; (中文(简体)). 单调表不能在模型中建模删除。 pv,且通知相对于更新的位置是一个建模选择,因为源头留给它自由.
- 推断结果以VFL相关性ID的私人函数为模型; 机器学习模型的质量以及分析方法的正确性都超越了象征性的证明.
- 请求的可获性、耐久性和成本不是模拟的,数据模型的个别识别资料(supis、 gpsis、 intGroupIds、 exterGroupIds)仅由受保护的请求机构代表。

主持人记录的是什么:

- 无答:K02.
- Z04,S05的答案依赖于该型号简化后的操作(附录D).
- 分析者为性质设定了攻击者条件，但既没有证明也没有攻击的（附录 D）：K02 在 `network` 下; K02 在 `rogue_nf` 下; K02 在 `stolen_token` 下。

- 没带对照查询的证明（附录 C）： A03: a03_resp, A03: a03_notif, A03: a03_acc, A08: a08, A08: a03_notif, Z01: a03_resp, Z01: z01_upd, Z01: z01_del, Z03: z03_upd, Z03: z03_del, K01: k01_tok, K01: k01_key, A08.9: a089, Z03.10: z03_upd, U01: a089。 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:应消费者本人要求作出的答复

每当 NF 消费者接受一次订阅创建/更新/取消的成功响应，就存在一个与之匹配的、由该消费者自己发起的订阅请求，且 subscriptionId、notifUri、notifCorreId 与请求中的值一致；每当 AF 发出一次通知，就存在一个此前由该消费者创建或更新、且 notifUri 与 notifCorreId 匹配的订阅。

AF只为消费者自己发出的请求开具订户,它发出的每一份通知都与该订户的notifUri和notifCorreId有关。 消费者只有在AF号机为自己的notifUri号机发送并携带自己的相关标识时才接受通知,因此结果不能从一个订阅转移到另一个订阅. 没有发现对任何一方的攻击。

- 结果:持有; 回答问题:是的; 可用备注
- 数值介质:约束是使通知可用于分析而无需混合订阅的方法; 证明与上面的运输并命令注意事项有关,而且单据上写明了程序,但没有写明这种财产。
- 在文件中说明:否
- 休息时间:TLS介于AF和每个NF是一个认证的信道; 回复和回调渠道由消费者创建并进入其内部。 ; 该通知是按以下方式制作的封存记录:AF/消费者会话键,与消费者的会话键核对notifCorreId. ; 通知相对于更新的位置是一个建模选择; 源头留给它自由。
- 开放:是否可以向消费者重播通知,假设是TLS,所以模型没有显示. ; 当通知在一次会话内重播时,哪一方的检查首先失败; 证明器对此财产没有控制权。
- 下一步:在对手所写的频道上模拟通知,将AF的会话认证作为唯一的寄件人检查,看看重播的InferNotif是否两次被接受.

A08:通知当地模式推论

每当 AF产生并返回/通知一次本地模型推理结果，该结果所携带的 VFL相关性ID与订阅中确定的 相关性ID一致，且通知发往该订阅的 notifUri并携带该订阅的 notifCorreId。

在这个分支中,AF人从其当地培训的ID相关模型计算结果,确定订阅,并在notifCorreId中将这一结果通知了订阅者notifUri。 因此,结果和订阅从未有好坏参半,除消费者之外,其他任何一方都不得从交易所中学习。

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:它是无VFL-客户分支的中心保障,它持有内部关联ID和密封运输的警示.
- 在文件中说明:否
- 参考:结果模拟为关联性ID的私人函数; 模型没有说分析的质量。 ; AF型机车与消费者之间的通道将通知封在会话键下。
- 开放:VFL相关ID系AF型机车内部承载,不在InferNotif型机车中承载,因此其通信是通过建筑而不是通过一个野外的消费者检查确定的.
- 下一步:检查后期发行是否带有结果中的关联性ID,这可以让消费者验证协会本身.

Z01:每次行动所需的有效代号

每当一个受保护操作（订阅创建、更新、删除，或通知被接受）被提交，提交方持有由 NRF 签发的、对该操作有效的 OAuth2 令牌；无有效令牌的请求不产生受保护副作用。

在模型中执行的AF每次受保护的操作,都是由持有访问信使的身份请求的,用于范围推论:在另一个NF名下的请求,用自己的信使创建、修改和删除任何内容。 单一服务范围涵盖整个API,因此范围本身区分了任何操作或资源; 身份检查确实如此。

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:6.4.9表示,使用OAuth2令牌授权访问,因此该要求是已知的; 2. 分析显示,身份检查是阻止NF号机以另一个名称行事,观众和过期部分开放的原因。
- 在文件中说明:是的。 文件上写着:s0272、s0273、s0275
- 休息:代号为每NF个代号的私人值,与请求中命名的身份代号进行等值核对。 ; AF型机车被信任进行核对; a 不诚实的AF按定义是无效的。
- 开放:信物的受众和过期要求不是模拟的; 模型检查 呼叫者持有 标志它命名的身份。 ; 创作主张没有记录控制权,因此没有迹象表明书面的这种财产在模型中会失败.
- 下一步:将信使作为由NRF人与主题,观众和到期人签名的断言模型,对另一个信使提出同样的询问.

Z03:托肯持有人是订阅创建者

每当一个令牌被用于更新或删除某个 subscriptionId 的订阅，该令牌的持有者就是该订阅的创建者（或经授权的实体），且令牌的受众为 AF； 令牌不能被用于其他订阅或其他操作。

只有当请求者是创建订阅的NF时,才适用更新或取消,因此带有自己有效标志的NF号无法触碰另一个NF的订阅. 保护依赖于AF的所有权检查,而不是范围,另外NF的代币的持有者是AF的NF,文件上称该代币为无记名证限额.

- 结果:持有; 回答问题:部分; 可用备注
- 价值介质:它隔离单一服务范围本身不保护任何东西,所有权检查携带财产; 失窃案件在文件中作了说明,只是部分模拟。
- 在文件中说明:是的。 文件上说: s0275
- 续:订阅标识符是AF生成的新值; 消息来源没有说它们是否可以预测。 ; 被泄露的脚趾攻击者没有过程作为代表,因此其行是检查的语句,而不是证明器跑去的攻击.
- 开放:信使的观众和不能用于另一操作的信使的说法不是模拟的. ; 在失窃的代币下,模型没有保存它的过程,所以行会说明支票是做什么的,而不是对证明器进行的攻击.
- 下一步:增加一个过程,持有一个泄露的令牌和一份已公布的subscriptionId,并询问它是否能够重新定位该订阅的notifUri; 这就是解决无记名者接触问题的方法。

Z04:未签署后无通知

每当一个订阅被成功删除（或 AF 以 termCause 终止），此后 AF 不再为该订阅发送新的通知，且针对该 subscriptionId 的更新不再生效。

在成功删除后,AF人拒绝为该订阅发出通知:链条保持新状态,通知尝试被拒绝. 证据取决于该状态被替换,控制显示:没有替换,通知被发送。

- 结果:在约束范围内持有(变化中的值未滚动为4步); 回答问题:是的; 可用备注
- 值介质:是保证不订阅停止报告,用控制机械显示在四个步骤停止的模型上.
- 在文件中说明:否

- 休息:生命周期未滚动为四个步骤:创建,删除,通知尝试,更新尝试. ; 状态是链条的位置,因为单音节表不能模拟删除.
- 开放:超过四个步骤后删除,以及两个同名消费者的订阅,都在未滚动模式之外.
- 下一步:扩展未滚动的链条,并添加同一消费者的第二次订阅,以查看一个删除是否给另一个留下了通知路径.

S05:未订阅后被拒绝的旧标识符

订阅删除生效之后， 使用旧 subscriptionId、旧 notifUri 或旧 notifCorreId 的请求不能触发新的通知或修改订阅。

一个仍然命名被删除订阅的标识符的请求不再修改,也不产生通知:删除后的更新尝试被拒绝,没有状态替换的控制接受. 消费者所保持的旧相关性 ID是模型之外。

- 结果:在约束范围内持有(变化中的值未滚动为4步); 回答问题:是的; 可用备注
- 数值低:在替换状态后从删除状态中产生; 值在于显示状态替换的控件是它携带的。
- 在文件中说明:否
- 休息:未滚动的链条比较更新前和通知前的状态. ; 主模型中的单调表无法显示去除,因此这个答案只来自未滚动的模型.
- Open: 请求在同一个消费者的新订阅存在的同时命名一个已删除的订阅是没有模型化的.
- 下一步:将一个消费者的两个订阅解开,并在删除其中之一时提出同样的问题.

K02:从其他NFs中保留目标身份和结果

订阅请求与通知中的目标身份（supis,gpsis,intGroupIds/exterGroupIds) 与推理结果只对发起订阅的消费者和 AF 可见， 其他 NF 与外部攻击者不能获得。

目标所说的情况是可以达到的:AF计算出当地模式的结果,签字的消费者得到并接受这种结果。 这一结果的保密性无法解决:ProVerif证实,只有消费者释放了该结果,攻击者才知道所通知的结果,但它无法为前提建立痕迹,所以所记录的答案是可达性,而不是秘密的证据. 结果被封在AF/消费者会话密钥下,所以只要该密钥停留在端点上,其他NF就无一读出来.

- 结果:仅可达到; 回答问题:部分; 无法使用
- 值低:证明器没有在微量级回答保密问题,所记录的可达性只表示交换发生.
- 在文件中说明:不明确。 资料来源:s0237、s0246。
- 休息:结果被封在AF/消费者会话密钥下; 释放结果的消费者在模型中是一个单独的身份. ; 保密查询在其前提上没有定论,因此这个目标没有证据级的答案.
- Open:保密查询已经核实,但验证者没有找到其前提的踪迹,因此答案基于一个过度近似. ; 目标身份(supis, gpsis, intGroupIds, exterGroupIds)作为保护请求体携带,不是模型中的个人值.
- 下一步:重新建立通知和消费者的清晰的每会状态,在一个工具中具体模拟会话,并在那里提出保密问题; 塔马林和特工就是这种情况。

K01:Token和TLS密钥从攻击者手中拿走

攻击者不能获得 NF 消费者的 OAuth2 访问令牌， 也不能获得消费者与 AF 之间 TLS 会话的密钥。

消费者的进入符和TLS会话密钥都没有被外部攻击者或另外的NF知道:它们是模型中的私人价值,没有信息携带. 这是其他结果所依据的假设,而不是协议的结果。

- 结果:持有; 回答问题:是的; 可用备注

- 价值低:它重申了整个分析需要证书和运输的假设,而单证已经要求运输。
- 在文件中说明:是的。 文件上写着:s0272,s0273
- 休息时间:按每NF人计的托肯和会话密钥为私人名称; 该模型不能证明原始人的计算强度。
- 打开:在NF号内存储令牌和会话密钥不是模拟的.
- 下一步:本模式无; 答案是其他结果所依赖的运输和证书假设。

A08.9:结果包含匹配的订阅和关联代号

每当 AF 返回或通知一次本地模型推理结果， 该结果所携带的 subscriptionId 与 vflCorrId 与该订阅创建/更新时确定的值一致。

消费者接受的结果是持有该消费者认购的notifCorreId和notifUri,因此结果附在正确的资源上。 subscriptionId号机车本身不在InferNotif号机车中,因此相关联是notifCorreId号机车和回调终点.

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:它是消费者所依赖的束缚,它告诫说,模型所束缚的识别符是关联的id,而不是订阅的URI.
- 在文件中说明:否
- 根据数据模型的定义,通知仅载有notifCorreId份通知和结果; subscriptionId号不在其中
- 公开:即时报告,即POST答复的结果而不是通知的结果,不是模拟的。
- 下一步:reportInfo型机车即时报告,并在201号回复中就结果提出相同的约束性问题.

Z03.10:没有交叉订阅更新或取消

一个持有自己合法 OAuth2 令牌的 NF 不能更新或删除另一个 NF 创建的订阅。

仅持有自己的代号的NF号机没有修改或取消另外NF号机型的订阅; 3. 每一次更新和取消都会与订阅时存储的拥有者对照检查,控制显示如果不进行这一检查,NF就可以取消另外创建的NF的订阅. 答案基于攻击者无法命名的标识符:模型给每个订阅一个新的标识符,所以确定的是所有权检查,而不是标识符的保密性.

- 结果:持有; 回答问题:部分; 可用备注
- 值介质:它显示单一服务范围留给AF人自己授权的,带有控制功能,并以文件没有做出的新识别器假设为基础.
- 在文件中说明:是的。 文件上写着:s0275、s0055、s0074
- 补习:订阅标识符是新鲜的、不可理解的值; 源代码未指定其生成。 ; 恶意的NF是一个脚本化的过程,所以只有写进模型的敌对请求才被尝试.
- 开放:交叉订阅攻击需要受害者的subscriptionId,这是模型中的新值; 源代码没有说明它是如何生成的。 ; 失窃案件没有过程作为代表。
- 下一步:让一个小偷处理被泄露的令牌,加上一个已公布的订阅费URI,并询问同样的所有权问题; 这就是单一范围变得明显的情况。

U01:更新后无停滞结果.

订阅更新生效之后， AF 返回或通知的推理结果不基于更新前的订阅配置； 更新前产生的旧结果不能与更新后的配置关联。

消费者在更新后接受的结果仍然是其notifCorreId和notifUri的订阅,更新没有改变。 消费者无法告知更新之前或之后计算结果:数据模型没有版本,因此这一部分依赖于AF重算以及消费者无法检查的任何内容。

- 结果:持有; 回答问题:部分; 可用备注

- 值介质:绑定部分持有,新鲜度部分识别文档未说明的数据模型中的一个空白; 2. 没有版本字段,无法向验证者询问新性问题。
- 在文件中说明:不明确。 资料来源:s0237、s0246、s0061。
- 休息时间:AF系仿照更新后的重算; 来源不要求这样做,而未说明飞行中的结果。 ; 该通知只载有notifCorreId和结果。
- 开放:InferNotif搭载没有版本或序列号,因此消费者没有检查显示在从之后生产的更新前产生的结果. ; 该型号的AF在更新后总是会重新计算,因此更新后交付的Stille results不是该型号的一部分.
- 下一步:在InferNotif上添加一个版本或reportInfo修订版,并询问AF号也可能在更新前提供计算结果的模型;这就是解决新鲜问题的方法。

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_resp			证明:6
A08	proved		a08			证明:4
Z01	proved		a03_resp			证明:6
Z03	proved		z03_upd	8中的6人		证明:8
Z04	bounded	未滚动到 4 步的数值变化	z04_notif	检查		2 已定界
S05	bounded	未滚动到 4 步的数值变化	z04_upd	检查		2 已定界
K02	reachable		运行			6 可达到
K01	proved		k01_tok			证明:4
A08.9	proved		a089			证明:2
Z03.10	proved		z03_upd	7中的6人		证明:7
U01	proved		a089			证明:2

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	每当AF为消费者代号创建个人推论订阅时,该消费者自己就用订阅数据(notifCorreId,notifUri)发送了与这些值的创建请求,所以subscriptionId以及消费者后来看到的关联字段都与自己的请求相匹配. 网外攻击者:无.	network	proved	a03_resp	无
A03	当AF人发出订阅通知时,该消费者会以通知中同样的notifUri和notifCorreId进行订阅。 网外攻击者:无.	network	proved	a03_notif	无
A03	只有在下列情况下,消费者才接受通知:AF已发出通知,说明notifUri拥有自己的notifCorreId因此,通知不归结为订阅错误。 网外攻击者:无.	network	proved	a03_acc	无
A03	每当AF为消费者ID创建订阅时,该消费者自己就发出带有这些价值的创建请求,尽管另外NF号拥有自己的有效标志. 网络外的攻击者:其自己的OAuth2号标语用于范围naf推论,以及其自己的TLS号标语,面向AF号标语.	rogue_nf	proved	a03_resp	无
A03	AF发送的每份通知都属于该消费者的订阅,匹配notifUri和notifCorreId,同样当另外NF个拥有自己有效代币的消费者消费API时. 网络外的攻击者:它自己的OAuth2表示范围naf推论,以及它自己的TLS身份对AF号.	rogue_nf	proved	a03_notif	无
A03	消费者只接受AF号为其notifUri号和notifCorreId号发出的通知,因此恶意的NF号消费者不能得到另一个消费者接受的关于自己所作决定的通知。 网络外的攻击者:它自己的OAuth2表示范围naf推断的标志,以及它自己的TLS身份朝向AF.	rogue_nf	proved	a03_acc	无
A08	AF号通知的每一项结果都是从当地训练有素的模型中计算出来的结果,用于确定VFL号订阅的关联性ID号,因此,结果和订阅不相上下。 网外攻击者:无.	network	proved	a08	无

目标	主张	攻击者	回答	查询	对照
A08	载有当地模式结果的通知涉及订户的notifUri,并附有订户的notifCorreId。 网外攻击者:无.	network	proved	a03_notif	无
A08	AF号通知的每一项结果都是计算出该订阅的关联性ID, 也是当另外NF号持自己的有效信使消费API号时。 网络外的攻击者:它自己的OAuth2表示范围naf推论和它自己的TLS身份.	rogue_nf	proved	a08	无
A08	其结果通知涉及notifUri的订阅费及其notifCorreId,甚至还有NF消耗了API. 网络外的攻击者:它自己的OAuth2表示范围naf推论和它自己的TLS身份.	rogue_nf	proved	a03_notif	无
Z01	在AF上创建订阅只针对其发送的命名身份请求,因此没有有效访问令牌的请求不会产生订阅. 网外攻击者:无.	network	proved	a03_resp	无
Z01	个人推论订阅的更新只针对签名人身份本身连同其签名人一起发出的请求。 网外攻击者:无.	network	proved	z01_upd	无
Z01	仅在签名人身份本身连同其签名人发出请求时,才删除个人推论的订阅。 网外攻击者:无.	network	proved	z01_del	无
Z01	AF号的订阅仅用于其名字中的身份请求,因此在另外NF号身份下展示自己的信物的NF号不产生订阅. 网络外的攻击者:它自己的OAuth2号标语用于范围naf推论和它自己的TLS身份.	rogue_nf	proved	a03_resp	无
Z01	更新只针对签名身份的请求,所以NF在另一个下方使用自己的标志NF身份改变不了任何东西。 网络外的攻击者:它自己的OAuth2参考范围及其本身的标志TLS身份证明。	rogue_nf	proved	z01_upd	无
Z01	删除只针对签名身份的请求,所以NF在另一个下方使用自己的标志NF'身份不删除任何内容。 网络外的攻击者:它自己的OAuth2参考范围及其本身的标志TLS身份证明。	rogue_nf	proved	z01_del	无
Z03	更新只代表发给该信物的身份,因此,另一个NF被盗信物的持有者被作为NF; 检查更新是由订阅的创建者 仍然持有在符号中的身份。 网络外攻击者:一个泄漏的OAuth2访问信物 合法的NF用于范围naf推论.	stolen_token	proved	z03_upd	无
Z03	(a) 删除只代表发出该令牌的身份; 在AF号上,失窃的证物使持证人成为同样的NF,这是有文件证明的无记名证限额,而不是对所有权的检查的中断。 网络外攻击者:一个泄漏的OAuth2访问信物 合法的NF用于范围naf推论.	stolen_token	proved	z03_del	无
Z03	订阅的更新仅代表创建该订阅的消费者进行。 网外攻击者:无.	network	proved	z03_upd	检查
Z03	订阅的删除仅代表创建该订阅的消费者进行。 网外攻击者:无.	network	proved	z03_del	检查
Z03	NF只持有自己的有效令牌,无法在另外NF的订阅上得到更新. 网络外的攻击者:它自己的OAuth2标志用于范围naf推论和它自己的TLS身份.	rogue_nf	proved	z03_upd	检查
Z03	NF只持有自己的有效令牌,无法再收到NF的订阅被删除. 网络外的攻击者:它自己的OAuth2标志用于范围naf推论和它自己的TLS身份.	rogue_nf	proved	z03_del	检查
Z03	更新只代表发给该信物的身份,因此,另一个NF被盗信物的持有者被作为NF; 所有权检查本身仍然持有 身份在符文。 网络外攻击者:一个泄漏的OAuth2访问信物 合法的NF用于范围naf推论.	stolen_token	proved	z03_upd	检查
Z03	(a) 删除只代表发出该令牌的身份; 失窃的物证使持证者在AF号上为NF,即无记名证限制文件状态。 网络外攻击者:一个泄漏的OAuth2访问信物 合法的NF用于范围naf推论.	stolen_token	proved	z03_del	检查
Z04	在成功删除其订阅(204 No Content)后,AF不再发出该订阅的通知:在未滚动的生命周期中,删除后的尝试被拒绝,只有在AF保持状态的状态仍然表示该订阅存在时才发出通知. 网外攻击者:无.	network	定界(变化中的数值未滚动为 4 步)	z04_notif	检查

目标	主张	攻击者	回答	查询	对照
Z04	AF在订阅成功删除之后,没有发出进一步通知,另外NF名持自己有效证书的人也消费API; AF所决定的状态 网络外的攻击者:它自己的OAuth2表示范围naf推论和它自己的TLS身份.	rogue_nf	定界(变化中的数值未滚动为 4 步)	z04_notif	检查
S05	成功删除后,一项命名旧的subscriptionId(其notifCorreId和notifUri)的请求不再修改订阅,也没有创建通知:在未滚动的生命周期上,删除后的更新被拒绝,而当国家仍然表示订阅存在时,则被接受. 网外攻击者:无.	network	定界(变化中的数值未滚动为 4 步)	z04_upd	检查
S05	在订阅被删除后,要求命名其旧的标识符不再修改,同样当另有NF人拥有自己的有效证书时也不再修改. 网络外的攻击者:其自己的OAuth2号标语用于范围naf推论,以及其自己的TLS身份.	rogue_nf	定界(变化中的数值未滚动为 4 步)	z04_upd	检查
K02	目标所述的情况是可以达到的:AF美元是当地训练有素的订阅模式的结果,用户接受和接受该模式; 这一结果的保密性是另一个说法,对此,证明器没有给出痕量级的答案。 网外攻击者:无.	network	reachable	运行	
K02	目标所述的情况是可以达到的,还有NF人消耗了API, 当地模式的结果到达了签字的消费者,并被接受。 网络外的攻击者:它自己的OAuth2标志用于范围naf推论和它自己的TLS身份.	rogue_nf	reachable	运行	
K02	目标所述的情况是可以达到的:当地模式的结果到达签字的消费者手中并被接受,而另一方持有一个泄露的信号。 网络外攻击者:一个泄漏的OAuth2访问信物,一个合法的NF用于范围naf推论.	stolen_token	reachable	运行	
K02	目标所述的情况是可以达到的:AF的计算是当地训练有素的订阅模式的结果,订阅者接受和接受这一模式。 这一结果的保密性是另一个说法,对此,证明器没有说明其前提。 网外攻击者:无.	network	reachable	reach_notif	
K02	目标所述的情况是可以达到的,而另外NF人拥有自己的资格,消耗了API:当地模式的结果到达了签字的消费者,并被接受。 网络外的攻击者:它自己的OAuth2标志用于范围naf推论和它自己的TLS身份.	rogue_nf	reachable	reach_notif	
K02	目标所说的情况是可以达到的,而另一方持有一个泄露的进入信号:一个当地模式的结果到达了签字的消费者,并被接受。 网络外攻击者:一个泄漏的OAuth2访问信物,一个合法的NF用于范围naf推论.	stolen_token	reachable	reach_notif	
K01	外部攻击者没有获得消费者的OAuth2访问令牌. 网外攻击者:无.	network	proved	k01_tok	无
K01	外部攻击者没有与AF号机一起获得消费者TLS会话的密钥. 网外攻击者:无.	network	proved	k01_key	无
K01	另外,持有自己有效证书的NF人没有获得消费者的进入证。 网络外的攻击者:其自己的OAuth2号标语用于范围naf推论,以及其自己的TLS身份.	rogue_nf	proved	k01_tok	无
K01	另外,持有自己有效证书的NF号机车无法与AF号机车一起获得消费者TLS会议的密钥. 网络外的攻击者:它自己的OAuth2号标语用于范围naf推论和它自己的TLS身份.	rogue_nf	proved	k01_key	无
A08.9	消费者接受的通知带有该消费者创建的订阅的关联性id和notifUri,因此结果与它的订阅有关. 网外攻击者:无.	network	proved	a089	无
A08.9	消费者接受的通知带有该消费者创建的订户的关联ID和notifUri,也是当恶意的NF消费者在场时。 网络外的攻击者:它自己的OAuth2标志用于范围naf推论和它自己的TLS身份.	rogue_nf	proved	a089	无
Z03.10	更新只是代表发给该信物的身份进行,因此一个泄露的信物使该信物的持有人为NF,即AF; 所有权检查本身仍然持有 身份在符文。 网络外攻击者:一个泄漏的OAuth2访问信物 合法的NF用于范围naf推论.	stolen_token	proved	z03_upd	无

目标	主张	攻击者	回答	查询	对照
Z03.10	订阅的更新只代表创建该订阅的消费者进行,所以其他任何一方都无法再修改NF的订阅. 网外攻击者:无.	`network`	proved	z03_upd	检查
Z03.10	订阅的取消只代表创建该订阅的消费者进行,所以其他任何一方都不能再取消NF的订阅. 网外攻击者:无.	`network`	proved	z03_del	检查
Z03.10	NF只持有自己的有效代币,无法更新另一个NF的订阅. 网络外的攻击者:它自己的OAuth2标志用于范围naf推论和它自己的TLS身份.	`rogue_nf`	proved	z03_upd	检查
Z03.10	仅持有自己有效证的NF号机不能取消另外NF号机的订阅. 网络外的攻击者:它自己的OAuth2标志用于范围naf推论和它自己的TLS身份.	`rogue_nf`	proved	z03_del	检查
Z03.10	注销只代表签发该令牌的身份; 泄露的物证使它的持有者NF现场AF中,即无记名控件限制文档状态。 网络外攻击者:泄露OAuth2合法访问符号NF用于范围参考。	`stolen_token`	proved	z03_del	检查
Z03.10	更新只是代表发给该信物的身份进行,因此一个泄露的信物使该信物的持有人为NF,即AF; 所有权检查本身仍然有效。 网络外攻击者:一个泄漏的OAuth2访问信物 合法的NF用于范围naf推论.	`stolen_token`	proved	z03_upd	检查
U01	消费者接受的结果与其创建的订阅有关:通知中标注的订阅额为notifCorreId,然后转到其notifUri,更新后没有变化,因此旧的结果不能用不同的配置标注. 网外攻击者:无.	`network`	proved	a089	无
U01	消费者接受的结果与其在更新后以同样的notifCorreId和notifUri创建的订阅有关,因此另外NF不能附加该订阅的结果. 网络外的攻击者:它自己的OAuth2号标语用于范围naf推论和它自己的TLS身份.	`rogue_nf`	proved	a089	无

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-20261115T000111, 2026-11-15. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:65,校对:10 s,壁17 min,耗资0.145 USD.

ProVerif:186 证明运行,182 决定,4 未答,6 s,58 答录.

分析了什么

协议	AF 推论 当地培训的模范分支
版本	19.2.0
分析范围	选 5.5.2.2.2明确允许的没有选中 NWDAFVFL客户仅用 AF本地已训练模型产生结果的分支；可信 AF与 NF消费者,一次订阅/更新/通知/取消。与多 客户端组合任务分别计为同一 API的不同配置。
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。 固定 Rel-19。分别区分外部网络攻击者与持有自身凭据的恶意合法 NF；TLS认证加密按端点建模，合法 NF不能读取其他 NF的 TLS会话。OAuth2主题/受众/范围/期限及 TLS身份绑定依照所附基线；服务 范围不自动等于资源所有权。单调表不能模拟真实删除，有限状态生命周期必须明确界定。目标是指定 API子流程，不是完整 5G安全。
原文	以下各节的318个编号段落(173955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	5.5	Naf_Inference 服务
主体	5.5.1	服务说明
主体	5.5.1.1	概览
主体	5.5.1.2	服务架构
主体	5.5.1.3	网络函数
主体	5.5.1.3.1	应用程序函数 (AF)
主体	5.5.1.3.2	NF 服务消费者
主体	5.5.2	服务业务
主体	5.5.2.1	导言
主体	5.5.2.2	Naf_Inference_Subscribe
主体	5.5.2.2.1	A. 概况
主体	5.5.2.2.2	推论订阅创建
主体	5.5.2.2.3	推论订阅更新
主体	5.5.2.3	Naf_Inference_Unsubscribe
主体	5.5.2.3.1	A. 概况
主体	5.5.2.3.2	推论订阅删除

文稿	章节	标题
主体	5.5.2.4	Naf_Inference_Notify
主体	5.5.2.4.1	A. 概况
主体	5.5.2.4.2	参考通知
主体	6.4	Naf_Inference服务 API
主体	6.4.1	导言
主体	6.4.2	使用费HTTP美元
主体	6.4.2.1	A. 概况
主体	6.4.2.2	HTTP标准标题
主体	6.4.2.2.1	A. 概况
主体	6.4.2.2.2	内容类型
主体	6.4.2.3	HTTP 个自定义标题
主体	6.4.3	资源
主体	6.4.3.1	概览
主体	6.4.3.2	资源:推论订阅
主体	6.4.3.2.1	说明
主体	6.4.3.2.2	资源定义
主体	6.4.3.2.3	资源标准方法
主体	6.4.3.2.3.1	POST
主体	6.4.3.2.4	资源自定义操作
主体	6.4.3.3	资源:个人推论订阅
主体	6.4.3.3.1	说明
主体	6.4.3.3.2	资源定义
主体	6.4.3.3.3	资源标准方法
主体	6.4.3.3.3.1	PUT
主体	6.4.3.3.3.2	PATCH
主体	6.4.3.3.3.3	DELETE
主体	6.4.3.2.4_2	资源自定义操作
主体	6.4.4	没有相关资源的自定义操作
主体	6.4.5	通知
主体	6.4.5.1	A. 概况
主体	6.4.5.5	推论通知
主体	6.4.5.5.1	说明
主体	6.4.5.5.2	目标 URI
主体	6.4.5.5.3	标准方法
主体	6.4.5.5.3.1	POST
主体	6.4.6	数据模型

文稿	章节	标题
主体	6.4.6.1	A. 概况
主体	6.4.6.2	结构化数据类型
主体	6.4.6.2.1	导言
主体	6.4.6.2.2	InferEventSubsc型机车
主体	6.4.6.2.3	InferEventSubscPatch型机车
主体	6.4.6.2.4	InferAnaSub型机车
主体	6.4.6.2.5	InferNotif型机车
主体	6.4.6.2.6	InferResult型机车
主体	6.4.6.3	简单数据类型和计数
主体	6.4.6.3.1	导言
主体	6.4.6.3.2	简单数据类型
主体	6.4.7	处理错误
主体	6.4.7.1	A. 概况
主体	6.4.7.2	协议错误
主体	6.4.7.3	应用程序错误
主体	6.4.8	特性谈判
主体	6.4.9	警卫
主体	6.4.10	HTTP 重新定向

协议的目的是在文档中将其定位为源步骤:选 5.5.2.2.2明确允许的没有选中 NWDAFVFL客户仅用 AF本地已训练模型产生结果的分支；可信 AF与 NF消费者,一次订阅/更新/通知/取消。与多 客户端组合任务分别计为同一 API的不同配置。

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	由消费者自己要求的答复	NF服务消费者(NWDAF)得到保证,它接受的订阅创建/更新/删除的每一个成功答复都符合它自己提出的要求,其中subscriptionId、notifUri和notifCorreId相同; AF保证其发出的每一份通知都属于消费者创建或更新的订阅,匹配notifUri和notifCorreId。	创建和更新程序配对 aHTTP联合国NF载有创建/更新的个人推论订阅资源和一个位置的响应服务消费者URI(s0040,s0049,s0055,s0061); 通知发送至notifUri从消费者那里收到的notifCorreId认购者数目(s0086); 数据结构将这两个字段定义为强制性的(s0237,s0246).	s0004, s0021, s0040, s0049, s0086, s0237, s0246

ID	简称	对象	文稿怎么说	出处
A08	与本地模型推论挂钩的通知	NF服务消费者得到保证,AF从其在无VFL-客户分公司接受过培训的当地ML型号所产生的结果就是为这一订阅而计算的(它确定为VFL相对应的ID和inferAnaSubs),并在该订阅的notifCorreId下交付给该订阅的notifUri。	s0048允许VFL服务器在选择无NWDAF VFL客户端时,从其本地训练的ML型号产生结果,该型号与已确定的VFL相关ID相关; 3. s0086要求通知前往对应订阅的notifUri,并携带InferNotif结构的notifCorreId(s0246).	s0048, s0086, s0246
Z01	每次操作所需的有效令牌	密码AF保证所有受保护的行动Naf_InferenceAPI(订阅创建、更新、删除)NF持有OAuth2对该项请求有效的访问令牌,没有这种令牌的请求没有受保护的副作用。	6.4.9声明进入Naf_InferenceAPI可由下列人士授权:OAuth2客户资格NRF作为授权服务器和该服务器NF服务消费者在消费服务前应先获得一个指示牌(s0272,s0273); 编号POST表格列表403禁止与将军SBI应用错误代码(E)s0143).	主机:7257, 主机:7259,s0272,s0273,s0143
Z03	Token 持有者为订阅创建者	AF型机车保证用于更新或删除给定的subscriptionId型机车的标志属于创建该订阅的NF型机车的消费者,该标志的受众是这AF型机车,该标志不能用于另一台机车的订阅或另一台机车操作.	API号界定了单一服务级别范围,没有资源或业务级别范围(s0275); 更新和删除程序针对个人推论订阅资源,其URI(s0055、s0074)和403紫禁是对资源方法(s0143)的界定答复; 任务范围指出,服务范围本身并不意味着资源的所有权。	主机:7263、s0275、s0055、s0074、s0143
Z04	未签署后没有通知	NF名服务消费者得到保证,在未订阅成功(204 No Content)后,AF不再发出订阅通知,对subscriptionId的更新不再生效。	Naf_Inference_Unsubscribe删除个人推论订阅资源(s0067,s0074),成功204 No Content(s0075); Naf_Inference_Notify报告了消费者订阅的活动(s0079,s0086); InferResult还允许AF号机车以termCause(s0249)请求终止.	s0067, s0074, s0075, s0079, s0086, s0249
S05	未订阅后拒绝的旧标识符	AF人可以放心,消费者可以信赖的是,要求仍然将旧的subscriptionId、notifUri或notifCorreId被删除的订阅命名为既不创建通知,也不修改订阅。	删除匹配subscriptionId(s0075,s0191)的个人推论订阅资源; 3. 仅向先前订阅的消费者发出有关notifUri和notifCorreId(s0086)的通知。	s0075, s0191, s0086
K02	目标身份和结果来自其他NFs	NF服务消费者得到保证,它于inferAnaSubs年发送的目标身份(supis, gpsis, intGroupIds, exterGroupIds)和收到的推论结果与其他NF消费者和外部攻击者保持了联系.	InferEventSubsc和InferNotif结构具有目标特征和结果(s0237、s0246、s0216); API是安全条款(s0272,s0275)中描述的基于服务的界面保护,任务范围要求一个合法的NF不能再读NF的TLS会话.	s0237, s0246, s0216, s0272
K01	Token和TLS 密钥从攻击者那里拿走了	密码NF服务消费者得到的保证是:OAuth2访问符号或TLS带有AF成为另一个人所知NF或者对外部攻击者。	6.4.9号为API号(s0272-s0274)的核准证书; 如TS 29.500(s0103 s0109)所述,API型机车达到HTTP以上,标准车头为HTTP,标准车头为TLS。	主机:7257, 主机:7259,s0272,s0273,s0103
A08.9	结果包含匹配的订阅和关联IDs	NF名服务消费者得到的保证是,AF回报或通知的每一项结果都带有subscriptionId和在创建或更新时为该订阅确定的关联性。	创建和更新程序使URI(s0049、s0061)所确定的个人推论订阅资源得到反映; 该通知载有相应订阅的notifCorreId(s0086,s0246),结果为订阅分析事件(s0248)的结果.	s0048, s0049, s0061, s0086, s0246

ID	简称	对象	文稿怎么说	出处
Z03.10	没有交叉订阅更新或取消	AF人可以放心,每个NF服务消费者可以信赖的是,只持有自己有效标志的NF不能更新或删除另外创建的NF订阅.	有1个服务级别范围,没有每个资源范围(s0275); 更新和删除地址:个人推论订阅资源URI(s0055,s0074)和403 紫禁用于资源方法(s0143); 任务范围规定,服务范围本身并不意味着资源的所有权。	主机:7263、s0275、s0055、s0074、s0143
U01	更新后无停滞结果	NF服务消费者得到保证,在更新订阅后生效后,AF回或通知的结果不是基于更新前的订阅配置,更新前产生的结果不能作为更新配置的结果.	AF00号卫星一旦成功,将相应更新目标个人推论订阅资源(s0061),并且该通知提供了订阅分析活动的结果和报告订阅信息(s0086、s0237、s0249)。	s0055, s0058, s0061, s0086, s0237

分析者没有补充性质：起草的清单已覆盖文稿写明的目标。

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 398 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 20 段，没选 378 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
P001 至 P002	rfc6749:2778-2786	没有陈述目标	OAuth威胁模型的前言和指针:不要求,也不攻击这个协议.
P003	rfc6749:2790-2795	K01	
P004 至 P006	rfc6749:2804-2823	不在范围内	本地客户和用户代理客户的客户密码和重定向URIs:NF-至NF客户证书的赠款类型不使用API。
P007	rfc6749:2827-2829	Z03, Z03.10, `rogue_nf`, `stolen_token`	
P008 至 P010	rfc6749:2831-2850	不在范围内	对授权服务器和资源所有者互动的要求; 两者都不是Naf_Inference分流的一部分。
P011	rfc6749:2859-2865	K01, K02, `network`	
P012	rfc6749:2867-2868	不在范围内	隐性赠款类型; Naf_Inference API号合同使用客户证书赠款(6.4.9)。
P013	rfc6749:2870-2872	Z01	
P014	rfc6749:2874-2877	Z03	
P015	rfc6749:2879-2881	Z03, Z03.10, `stolen_token`	
P016 至 P021	rfc6749:2885-2917	不在范围内	刷新令牌: 这里使用的客户证书授权没有 。
P022 至 P029	rfc6749:2921-2980	不在范围内	授权代码授权和重定向 URI操纵: 赠款类型和用户代理流量 API没有使用.
P030 至 P033	rfc6749:2984-3003	不在范围内	资源所有者密码证书授权:本API没有使用.

段落	出处	定为	不选的原因
P034 至 P035	rfc6749:3013-3019	K01, K02	
P036	rfc6749:3023-3028	K01	
P037 至 P039	rfc6749:3032-3041	没有陈述目标	猜测授权服务器上的客户端密码:这个API没有带客户端密码,而令牌的发行不在选定的子流之外.
P040 至 P048	rfc6749:3045-3110	不在范围内	盗版和跨站点请求伪造:用户代理流,非NF-至NF API.
P049 至 P050	rfc6749:3119-3138	不在范围内	点击劫机:用户代理流.
P051 至 P052	rfc6749:3142-3150	不在范围内	授权服务器自身输入中的代码注入: 不是这个API.
P053 至 P054	rfc6749:3154-3167	不在范围内	在授权端点打开重定向器:不是这个API.
P055 至 P062	rfc6749:3170-3210	不在范围内	滥用赠款的隐性:API没有使用的赠款类型。
P063	ts-33-501:2491-2491	不在范围内	下标AS/NAS安全算法:RAN级,而非Naf_Inference次流.
P064 至 P072	ts-33-501:2495-2511	不在范围内	认证和授权5G核心的UE:任务范围是Naf_Inference API子流,而不是整个5G安全架构.
P073 至 P074	ts-33-501:2515-2517	不在范围内	5G核和NG-RAN的密钥:API子流外.
P075 至 P078	ts-33-501:2523-2529	不在范围内	空中接口一般用户数据保护.
P079 至 P089	ts-33-501:2533-2553	不在范围内	RAN型机车的用户和信号数据保密性; 2. API的有效载荷保护是K01和K02在TLS任务范围假设下提出的。
P090 至 P103	ts-33-501:2557-2583	不在范围内	RAN型机车的用户和信号数据完整性.
P104 至 P110	ts-33-501:2587-2599	不在范围内	UE和UICC号机的订阅全权证书的存檔。
P111 至 P125	ts-33-501:2603-2631	不在范围内	订户隐私(SUCI,SUPI隐匿)在空中接口和核心内; 4. API的目标身份在TLS-保护订阅请求(K02)中携带。
P126 至 P178	ts-33-501:2637-2761	不在范围内	gNB,ng-eNB,F1和E1的要求:无线电接入,该系统的一部分,这一任务被排除在外.
P179 至 P196	ts-33-501:2767-2805	不在范围内	AMF NAS- 标注保密性,完整性和订户隐私:不是API子流.

段落	出处	定为	不选的原因
P197 至 P213	ts-33-501:2809-2853	不在范围内	SEAF,UDM,AUSF和UDR所需经费:UE型机车的认证和订阅数据.
P214	ts-33-501:2859-2859	`rogue_nf`	
P215	ts-33-501:2865-2865	不在范围内	NF的发现和注册的回放保护; 假设订阅费API不要求重播。
P216 至 P217	ts-33-501:2867-2869	不在范围内	NRF 授权发现和地形隐藏:发现,不是这个API.
P218	ts-33-501:2871-2871	A03, Z01, `network`	
P219	ts-33-501:2873-2873	Z01, `network`	
P220	ts-33-501:2875-2875	A03, Z01	
P221 至 P227	ts-33-501:2879-2891	Z01	
P228 至 P234	ts-33-501:2895-2907	不在范围内	外部曝光的NEF安全要求:这个API的无人信任的AF配置,与这里的可信任的AF分支不同.
P235 至 P241	ts-33-501:2911-2923	不在范围内	服务通信代理:间接通信,被任务范围排除在外.
P242 至 P254	ts-33-501:2929-2953	不在范围内	PLMN通信与SEPP:单机操作器API子流外.
P255 至 P303	ts-33-501:2957-3055	不在范围内	SEPP和漫游的中介要求:在下流之外.
P304 至 P312	ts-33-501:3059-3075	不在范围内	跨越N32的属性保护:漫游界面.
P313 至 P314	ts-33-501:3079-3081	不在范围内	IPUPS要求:边境保护,分流外.
P315 至 P318	ts-33-501:3085-3091	不在范围内	创建网络标识符头用于漫游:在子流外.
P319 至 P327	ts-33-501:3097-3115	不在范围内	信号监测配置和流线:在子流外.

段落	出处	定为	不选的原因
P328 至 P337	ts-33-501:3121-3141	不在范围内	运营商的安全能见度和配置要求:部署,而非API型.
P338 至 P369	ts-33-501:3149-3215	不在范围内	NAS密码学和完整性算法识别器及选择:RAN/NAS,API的TLS套套房的强度是无法向证明器询问的.
P370 至 P398	ts-33-501:3219-11901	不在范围内	5G-RG、NSSAAF、N3、EAP-TLS、IAB、MBS和NEF附件要求:本任务不包括的系统部分。

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 23 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 3 项，没设的 20 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	NF 服务消费者	参与方	`rogue_nf`	
S02	AF	参与方	按定义全部失守	AF型机车产生当地模式的结果,看到每个标志,是执行授权和所有权检查的一方; a不诚实的AF按定义全部无效,这个分支的范围将AF修复为可信赖的(可信 AF),无人信赖的变体是NEF配置.
S03	NRF	参与方	按定义全部失守	敌对的授权服务器可以为任何NF个身份设计一个有效的代号,因此这里要求的每一个授权财产都按定义失败; 这两份文件在一份已失密的NRF(33.501 5.9.2.2有NRF和NFs相互认证)下没有提出任何要求。
S04	其他 NF	参与方	`rogue_nf`	
S05	外部攻击者	参与方	攻击者得不到更多	外部攻击者是拥有网络而无其他的攻击者; 攻击者默认为每个目标都在场 并且没有任何东西在网络之外, 所以没有进一步的攻击者从它。
S06	subscriptionId	值	攻击者得不到更多	密码subscriptionId是给其内部的订阅者的资源标识符TLS届会; 知道一个人没有能力,因为AF授权由调用者的代号以及该资源的存储所有者进行更新或删除,这就是Z03财务报告和财务报告Z03.10询问和所有权查询显示什么 。
S07	notifUri	值	攻击者得不到更多	接受通知并不取决于是否知道notifUri:通知机构是根据AF/消费者会话密钥密封和认证的,必须携带消费者自己的notifCorreId(A03),因此,只知道URI的一方一无所获。
S08	notifCorreId	值	攻击者得不到更多	notifCorreId与AF/消费者会话密钥下的通知的封条一起检查,因此仅知道一个关联的id就不允许缔约方提出可接受的通知(A03)。
S09	订阅内容	值	攻击者得不到更多	订阅内容只说另一个消费者要求的; 它没有能力修改订阅或接收其结果,两者都需要所有者代币(Z03,Z03.10)。
S10	vflCorrId	值	攻击者得不到更多	VFL相关ID由AF确定,用于选择本地模式; 3. 知道它不会产生结果,这出自AF的私人型号(A08).
S11	本地已训练 ML 模型引用	值	攻击者得不到更多	提到AF的当地训练的模型是名字,而不是秘密; 该型号仅在AF型机车内使用.
S12	推理结果	值	攻击者得不到更多	持有一个推论结果没有进一步的能力:通知被封存给订阅者,并绑定其自己的关联ID,因此结果不能变成一个被接受的通知(A03,A08)。
S13	OAuth2 访问令牌	值	`stolen_token`	
S14	(a) 参考范围	值	攻击者得不到更多	服务范围是界定整个API的公开标签; 它本身没有授权, 符号是(Z01)。

ID	参与方或值	类别	攻击者条件	不设的原因
S15	订阅资源	值	攻击者得不到更多	订阅资源为AF美元; 持有其陈述书或第URI号陈述书副本,没有所有人证明书就无法更改其陈述书或收到其通知。
S16	订阅状态	值	攻击者得不到更多	订阅状态通过存在和所有者检查每一次更新和删除,在AF强制执行; 知州无能. 成功删除后的状态会在未滚动的模型中解答,因为单音表不能删除一行.
S17	通知	值	攻击者得不到更多	通知是AF/消费者会话密钥下密封的密钥; 持有一个不能给出任何能力超出它所携带的结果, 和重播 具有相同的结果 和相同的关联ID。
S18	苏皮斯 Supis	值	攻击者得不到更多	目标身份(supis, gpsis, intGroupIds, exterGroupIds)表示谁是分析订阅者; 持有它们无法订阅、取消或收到结果,K02要求这样做。
S19	gpsis (英语).	值	攻击者得不到更多	目标身份(supis, gpsis, intGroupIds, exterGroupIds)表示谁是分析订阅者; 持有它们无法订阅、取消或收到结果,K02要求这样做。
S20	intGroupIds	值	攻击者得不到更多	目标身份(supis, gpsis, intGroupIds, exterGroupIds)表示谁是分析订阅者; 持有它们无法订阅、取消或收到结果,K02要求这样做。
S21	exterGroupIds	值	攻击者得不到更多	目标身份(supis, gpsis, intGroupIds, exterGroupIds)表示谁是分析订阅者; 持有它们无法订阅、取消或收到结果,K02要求这样做。
S22	TLS 会话密钥	值	不在范围内	任务范围表示,符号模型不能证明计算安全性:持有TLS会话密钥的攻击者是分析所忽略的破旧攻击者.
S23	订阅配置	值	攻击者得不到更多	订户配置由AF人及其所有者掌握; 明知它没有改变它的能力,这需要拥有者的代币,也没有能力获得另一个订阅的结果.

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		
`rogue_nf`	合法的NF服务消费者自持证:NRF号机为单机范围"naf-information"(6.4.9)发行的OAuth2访问证,其面向AF号机的TLS身份,以及其自主的API根URI空间; 3. 它不能读取其他NFs的TLS会话(任务范围).	6.4.9说,可授权使用OAuth2客户证书,这是整个服务范围之一(s0272、s0275); 任务范围将外部网络攻击者与持有自己证书的恶意合法NF区分开来.	主机:7257,主机:7263,s0272,s0275
`stolen_token`	向合法NF名消费者发放的OAuth2访问证,用于范围"纳夫推断",并已泄露给该消费者; 4. 它可以通过自己的连接在服务请求中显示该符号。	6.4.9做一个OAuth2用于访问的证书 Naf_Inference(s0272-s0274);RFC674910.3(线条)2879-2881说明该规格没有给资源服务器任何方法,以确保向其出示的令牌是发给该介绍人的,并要求在过境和储存时对访问令牌保密(行)。 2859-2865).	主机:7257,rfc6749:2879,s0272,s0273,s0274

ID	`network`	`rogue_nf`	`stolen_token`
A03	成立	成立	
A08	成立	成立	
Z01	成立	成立	
Z03	成立	成立	成立
Z04	成立	成立	

ID	network	rogue_nf	stolen_token
S05	成立	成立	
K02	无答案	无答案	无答案
K01	成立	成立	
A08.9	成立	成立	
Z03.10	成立	成立	成立
U01	成立	成立	

关于证明和模型的说明

- Z04:在ProVerif中回答,分析师的名字是changing_state。
- S05: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
subscriptionId是否仍然表示现有的个人推论订阅,由谁拥有	用于每个推论订阅资源的AF(VFL服务器)	a 订阅由成功的POST(201 Created,s0049)创建,由成功的PUT/PATCH(s0061)取代,以成功的DELETE(s0075)结束.	在每PUT/PATCH或DELETE次命名subscriptionId之前,在发出订阅通知之前(s0086次); 在模型中。 pv 检查是存储订阅上的存在和所有者查询	s0049, s0055, s0061, s0074, s0075, s0086
第notifCorreId号和第notifUri号协议,对订阅书有约束力;	NF服务消费者(notifCorreId和notifUri后面的回调终点)和AF(notifUri和notifCorreId储存供订阅)	创建请求(s0040、s0237)和每一份更新请求(s0055、s0058)	根据消费者收到的每份通知:InferNotif携带的notifCorreId必须是该消费者的订户,而且通知必须在AF/消费者会话密钥下开放。	s0086, s0237, s0246

模式	结果	目标	显示于ProVerif	步骤
repeat_one_time_action	没有找到			锁链在界内。 pv 拒绝删除后的第二次操作; 型号。 pv的单调表会接受重复的DELETE,因为一行不能被移除,这是工具的极限,而不是协议的极限.
重播(E)	没有找到			InferNotif搭载没有序列号或时间戳(s0246),消费者只比较了notifCorreId(s0086),因此网络重播的相同通知会被接受两次. 任务范围模型TLS作为端点之间的认证加密,这阻止了记录的重播,因此这停留在TLS假设之内,没有突破目标:对此没有要求查询.

模式	结果	目标	显示于 ProVerif	步骤
脱同步	没有找到			消费者和AF人通过notifCorreId号协议订阅,但更新没有改变,并通过notifUri号协议订阅AF商店和用途; 由于每次更新和删除都会在应用前与存储的拥有者核对,所以无法通过源代码允许的一条消息使当事人所保存的对数值发生差异。
update_before_check	没有找到			AF 仅在存在和所有者检查存储订阅后回答更新或删除; z03_upd和z03_del显示,除创作者外,没有进行更新或删除.
no_rollback_on_failure	没有找到			一次被拒绝的通知尝试和删除后被拒绝的更新使得AF的状态处于限定状态. pv:拒绝发出AfRefusedNotif和AfRefusedUpd,不将链条移回直播状态.
race_between_sessions	没有找到			每一份申请都要通过消费者为它创建的答复渠道进行,AF检查了它所提供subscriptionId的存储所有者; 两位消费者同时行动不能改变对方的订阅,如z03_upd和z03_del对恶意NF的显示.
distinguishable_failure	没有找到			来源将拒绝更新或删除的错误代码留给第6.4.7条(403或404),两者都只回答呼叫者; 模型不建模错误体,所以无法得出任何关于探测器的结论,该探测器可以将现有的订阅从不存在的订阅中看出出来. subscriptionId是AF生成的新鲜值,只给订阅者,因此这样的探测器首先需要识别符.
wrap_or_window	没有找到			没有计数器,序列号或验收窗口保存:唯一更改的值是订阅是否存在,其两个值由定界链处理. PV,所以没有东西可以包围。

分析师给目标取了什么名字?

步骤	目标	特性	原因：
51	Z04, S05	changing_state	Z04和S05取决于AF为每个个人推论订阅所保持和更改的价值:订阅是否仍然存在。 模特儿时 pv 订阅表为单调(一行不能删除),因此成功删除对后期通知和后期更新对命名旧subscriptionId的影响被解围. pv到四个步骤(创建,删除,通知尝试,更新尝试),在通知或更新被接受之前与状态进行比较.

分析员的结语

11个目标被信任的...AF,本地模式分支Naf_Inference(TS29.572v19.2.0),无结论:协议给出了所分析假设中的目标要求.

由模型上的证据建立. pv(任何会议次数):AF只为消费者自己请求而订户,仅通知该订阅的notifUri和notifCorreId(A03); 该通知的结果是计算出该订阅的关联性ID(A08),消费者只接受以AF/消费者会话(A08.9)封存的关于其自身关联性id的通知; 每个创建、更新和取消都由持有naf-inform 代号(Z01)的身份要求; 更新或取消只代表订阅者的创建者适用,而伪造的控制(ctl_z03)显示支票是其携带的(Z03,Z03.10); 和TLS密钥留在消费者身边(K01); 更新后的结果仍受订阅的约束(U01,绑定部分).

建立于界限。 pv,订阅生命周期未滚动为四个步骤,每个步骤都有伪造的控制:在成功删除后,AF既不通知也不应用该订阅的更新(Z04,S05)。

例如,微弱的答复:推断结果的保密性(K02)只记录在可达到的程度,因为ProVerif核实了暗示,但没有找到其前提的痕迹; 由于InferNotif没有版本或序列号,因此U01的新鲜度主张依赖于AF重算,因此在更新后完全不能询问这种数据模型的新鲜度。

块和限制:恶意NF和令牌-thief案件是脚本程序,而不是自由的对手计算,订阅标识符是源代码未指定的新鲜值,TLS和OAuth2被作为声音(一个破碎的原始键或漏出的会话键超出了范围),一个单调表强迫删除属性进入受约束的模型. 六份证明(A03,A08,A08.9,Z01,K01,U01)没有控制查询. K02的保密问题和通知前后的每会状态是Tamarin与一名特工的案件.