审查培训活动的安全分析

19.8.0 — ProVerif+ 代理 报告

文稿	5G系统; 网络数据分析服务; 阶段3(协议定义）; 5G系统的安全结构和程序(辅助))
检查的性质	12 条：4 条成立，8 条不成立（8 个攻击）
发现	3

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

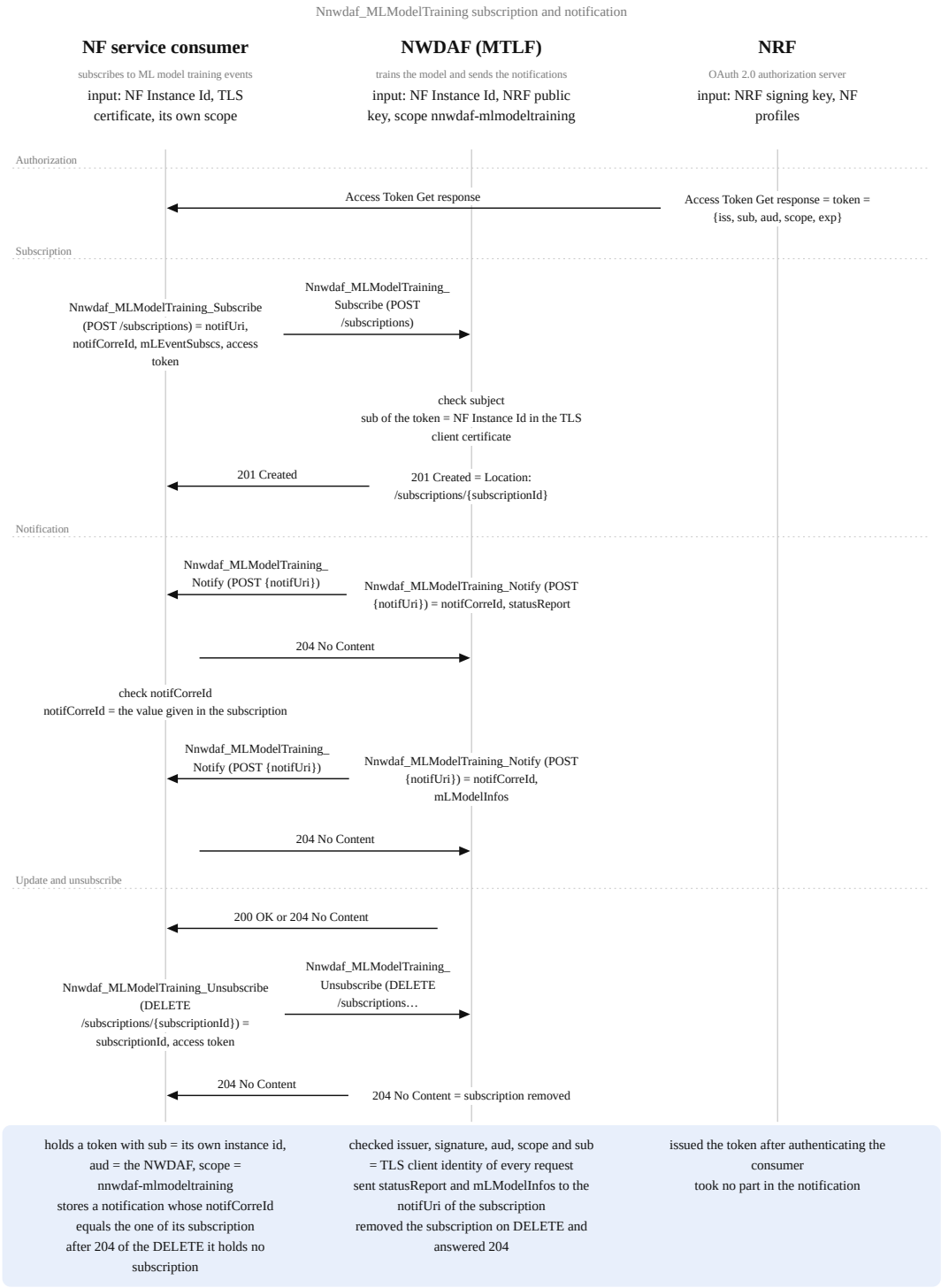
Nnwdaf_MLModelTraining服务让NF服务消费者要求包含MTLF的NWDAF培训ML型号:消费者订阅ML型号培训活动,可能更改订阅,收到回调URI的通知,不订阅. 双方是消费者,NWDAF,以及NRF,它们发行了OAuth 2.0访问令牌,授权NF使用服务.

在订户结束时,消费者知道哪一个是NWDAF例接受的,而且每一份它接受的通知都是哪一种。 NWDAF号知道NF号协议的签署,即召回URI号协议的签署,而且请求中还附有发给该申请的这项服务的代号。

双方:

- **NF服务消费者**:订阅ML示范培训活动. 持有量:NF exactence Id,TLS 证书,其范围.
- **NWDAF(MTLF)**:训练该型号并发送通知。 持有:NF exactence Id,NRF 公钥,范围nwdaf-mlmodeltraining.
- **NRF**: OAuth 2.0 授权服务器. Holds: NRF 签名密钥, NF 简介.

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3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。

该服务授权并关联了有文件记载的订阅,但通知路径没有经过API定义的字段验证,所以一个合法的NF可以推动NWDAF从未发送的通知. 另有两个缺点:由于API定义了不通知例,而且订阅资源没有授权,所以在重播后可以再次接受通知,因此任何NF持有服务符,subscriptionId可以删除或改写另一个消费者的订阅. 在消费者之间孤立训练有素的模型,不利于网络,也不利于另一个消费者。 包装两页:将发送者身份与订阅的NWDAF进行对比,以关闭第一个弱点,并添加一个通知序列号以关闭第二个弱点; 信号失效,通过SCP号机的间接通信以及DELETE号机后的飞行通知不在模型之外.

攻击数字采用图1的列数. 红色是攻击者的行为. 黄色标记了一方发送的信息,尽管指定的交换点当时没有它,以及攻击中断的结果.

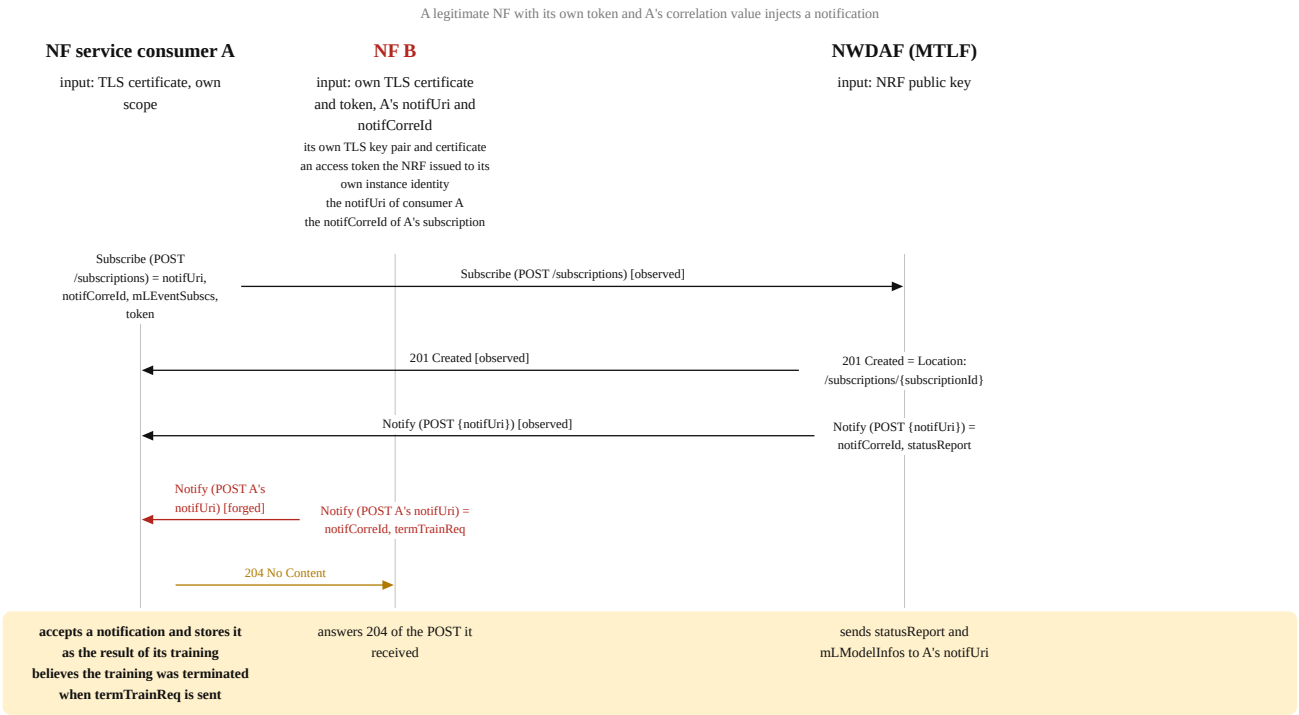
2.1 合法NF号可以发送从未发送的NWDAF号通知

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	高
涉及的性质	A02, D01, U01, Z05, Z05.12 （见第 3 节）
原文	s0129, s0321, s0138, s0445
依据	ProVerif 攻击询问 `a02l`,`u01l`; 图2、3、4、5和6

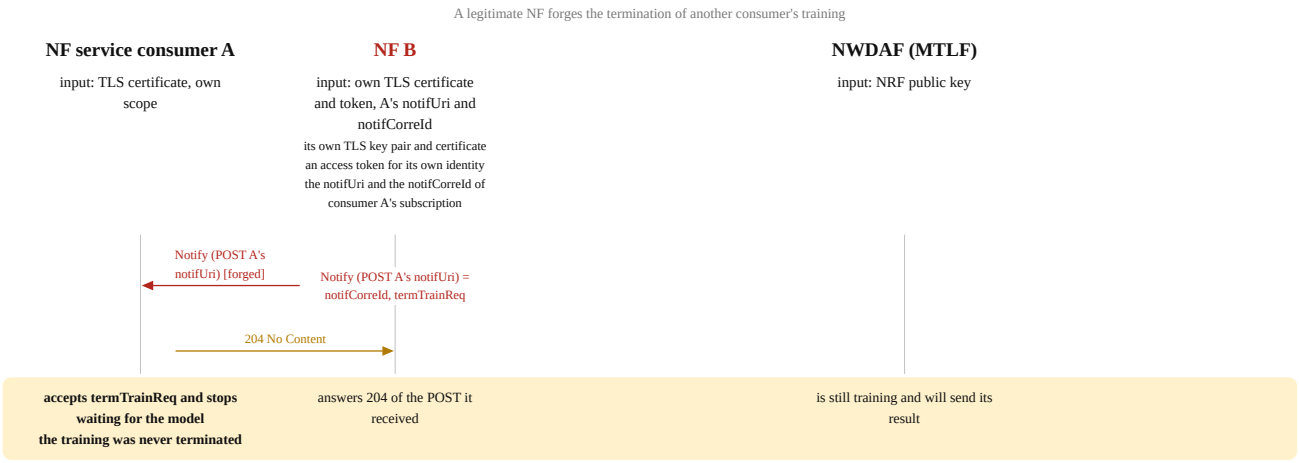
发生了什么。 通知业务不包含在OAuth2.0中,API要求消费者只需检查notifCorreId等于其订阅价值. 确切地检查了接受POST的消费者,从任何NF个知道URI和相关价值的例子中调回URI,并且通过自己的训练储存尸体.

攻击者需要什么。 登记在案的NF00个案件,有其自己的TLS份证书,受害人消费者的notifUri份证书及其notifCorreId份证书; 两者都是消费者选择的价值观,规格不需要保密。

攻击者能得到什么。 攻击者决定受害者对从未发生的训练的看法:一个虚构的模型位置,一个虚构的状态报告,或一个termTrainReq,使得受害者不再等待它的模型.



- 图2。 合法的NF 带有自己的标志,A的关联值注入了通知. 财产A02; 攻击查询 a02l。 *



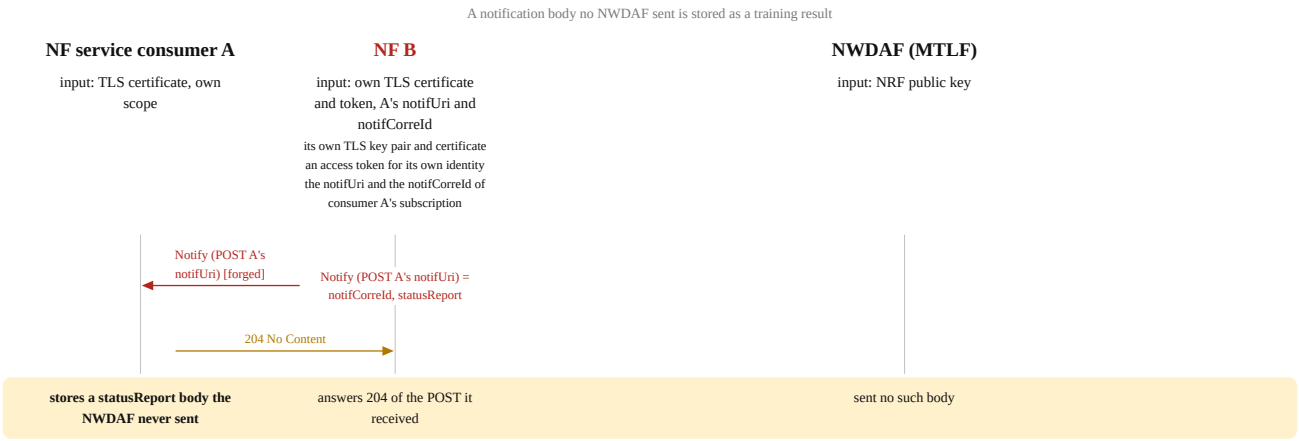
- 图3。 合法的NF伪造终止另一个消费者的培训. 财产U01; 攻击查询 u01l。 *



- 图4。 外国的结果达到了消费者的回调 URI。 财产Z05; 攻击查询 a02l。 *



- 图5。 外国ML程序的结果被接受为A自己的结果. 财产Z05.12; 攻击查询 a02l。 *



- 图6。 作为培训结果,已存放了第NWDAF号通知机构。 财产D01; 攻击查询 a02l。 *

拟议修改。 要求消费者比较经认证的TLS通知的客户身份POST与NF实例ID会 议 日 程 和 议 程NWDAF并且当通知不同时拒绝通知。 该模型的验证消费者完全进行这种比较:与之相比,验证查询被持有,伪造的通知被拒绝。

用 ProVerif复核。 修改内容已输入模型副本:消费者比较经认证的SBA通知中的身份NF案件编号NWDAF并拒绝通知,而不是只检查notifCorreId等于订阅值。ProVerif仍然发现攻击为`a02l`: 更改不删除它. 协议的正常运行仍然被找到. 在其它有记录的答案中,16仍然坚守1已更改 :`u01l`(U01现在已经核实。 已更改模式 :`records/fixes/0068-fix-sender.pv`.

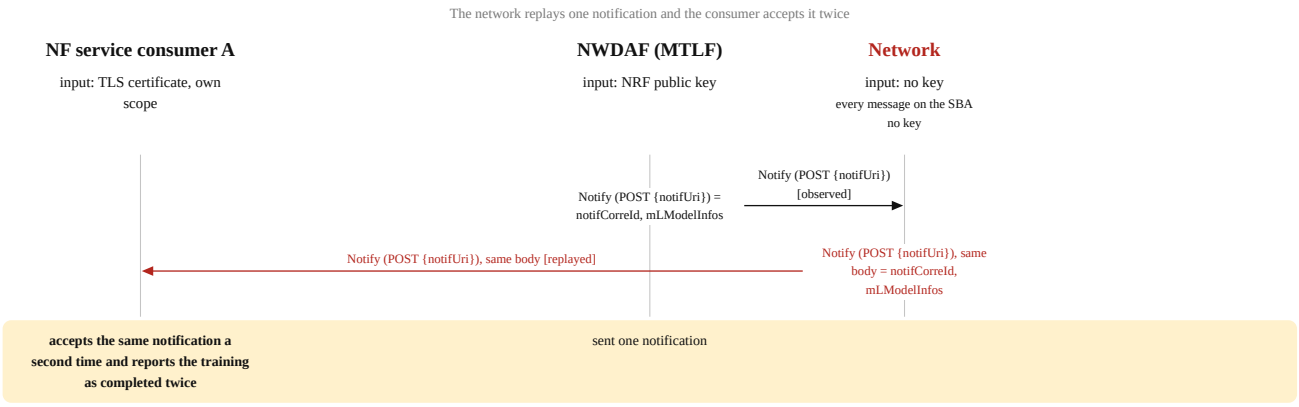
2.2 重复播放时再次接受通知

类型	协议规范本身的弱点
是否新发现	是：文稿里没有写到
价值	高
涉及的性质	A04, A04.10 （见第 3 节）
原文	s0129, s0321
依据	ProVerif攻击查询`a04`; 图7和8

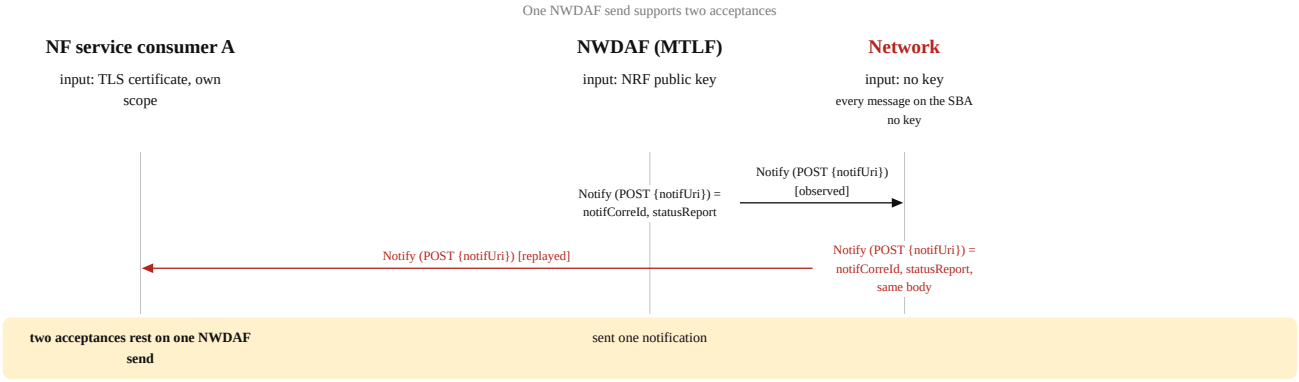
发生了什么。 NwdafMLModelTrainNotif带有订阅的关联标识符,没有通知实例或序列号。 消费者不能告诉第二次交付它从新通知中已经接受的通知,而分享notifCorreId的同一NF的两次订阅是无法区分的,因此接受另一个通知。

攻击者需要什么。 只有网络:从电线上取出通知并再次交付,或者以同样的notifCorreId第二次订阅同一NF例.

攻击者能得到什么。 消费者重复一份状况报告或完成情况报告,并混淆其自己订阅的通知; NWDAF的状态和消费者对训练的看法不一,两边都没有出错。



- 图7。 网络重播一次通知,消费者接受两次. 财产A04; 攻击查询 a04. *



- 图8。 1个NWDAF发送支持两个接受. 财产A04.10; 攻击查询 a04。 *

拟议修改。 每份订阅通知增加一个订阅通知序列号为NwdafMLModelTrainNotif,每份订阅通知增加NWDAF,并要求消费者拒绝其已经接受的价值和低于上次接受的价值。 序列号必须由NWDAF设计:通知关联标识符由消费者选择,不能作为实例标识符.

用 ProVerif 复核。 未核对:消费者将保留最后接受的号码,这一数值随每次通知而变化; 需要未滚动的订阅生命周期模型,而本分析中并未构建该模型,因此在不进行验证检查的情况下,提出修改。

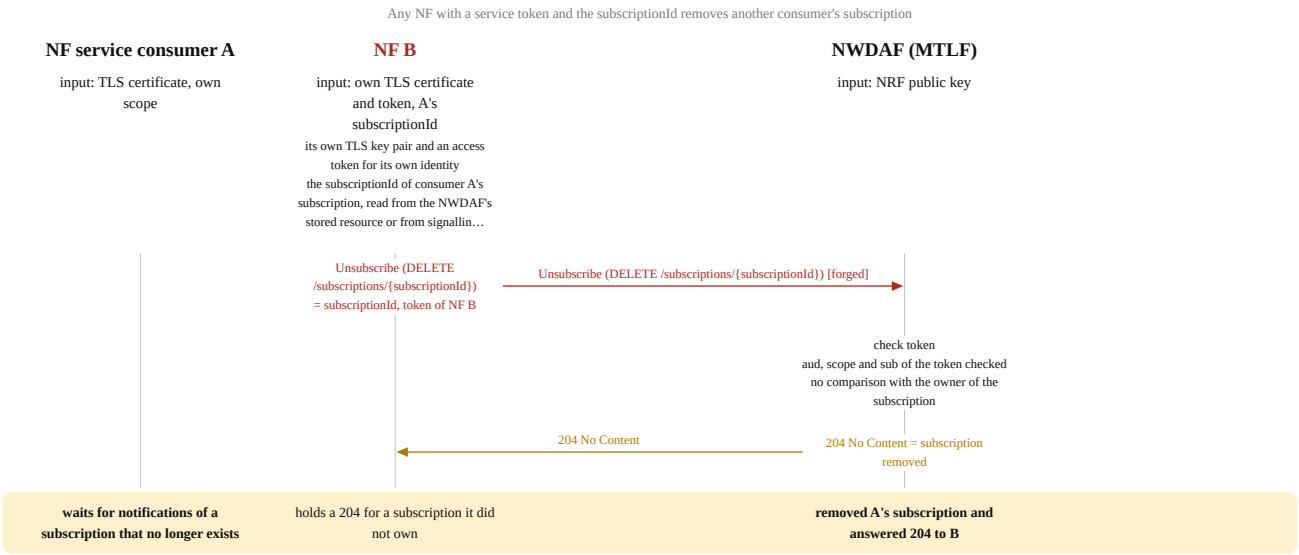
2.3 订阅资源本身没有授权

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 (主要为:492)
价值	高
涉及的性质	A03 （见第 3 节）
原文	s0378, s0442, s0105
依据	ProVerif攻击查询`a03b`; 图9

**发生了什么。页:1API界定整个服务的单一范围,没有资源一级的范围,以及NWDAF行为subscriptionId名称URI对于任何出示有效证物的消费者。 再来一次NF实例知道subscriptionId,它可以取消订阅或重写,例如通过替换notifUri.

攻击者需要什么。 正当的NF以它自己的象征,subscriptionId受害人的订阅,从NWDAF或从信号监视器。

攻击者能得到什么。 攻击者默默地取消另一消费者的训练,或将包括训练有素的型号在内的未来通知转回自己的URI。



- 图9。 任何带有服务标志的NF和subscriptionId都会取消另一个消费者的订阅. 财产A03; 攻击查询 a03b. *

拟议修改。 界定一个额外的范围,将消费者可能处理的资源命名为:TS33.501已经允许,并需要NWDAF将访问标志的主题和额外范围与创建该标志的消费者进行比较。subscriptionId在此之前PUT,PATCH财务报告和财务报告DELETE.

用 ProVerif 复核。 未核对:该型号仅包含服务级别范围; 附加范围主张和NWDAF与所储存所有者的比较是象征性内容的改变,超出了所分析的基准。

没有发现这些攻击事件的数字:A02:u01l,D01:u01l,U01:a02l,Z05.12:u01l,Z05:u01l。

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
A02	**经认证的请求和通知同行。** 每当 NWDAF 接受某消费者实例的订阅/更新/取消请求，或消费者接受 NWDAF 的通知，声称的对端必须确实以本方为对象运行过该协议。	无	不成立（1 个攻击）	高	不确定
A03	**通知和订阅关系。** 消费者接受通知时，须存在匹配的自身订阅运行，notifCorreId、notifUri、mlCorreId、roundInd 一致；NWDAF 接受更新/取消时，subscriptionId 须属于该消费者。	无	不成立（1 个攻击）	高	不确定
A04	**每项通知活动均接受一次。** 消费者对同一通知实例至多接受一次；若规范无序号字段，则须显式记录该性质不可由规范字段保证。	无	不成立（1 个攻击）	高	否
D01	**通知有效载荷完整性。** 消费者接受的每条通知，其发送方为订阅的 NWDAF，且 mLModelInfos、statusReport、termTrainReq 等载荷与 NWDAF 实际发送一致。	无	不成立（1 个攻击）	高	不确定
K01	**长期证书保密。** 攻击者不能推导 NRF 的令牌签名私钥或任一 NF 的长期认证凭据。	无	成立	低	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
Z01	**服务访问需要有效的符号。** NWDAF提交订阅/更新/取消操作时，须存在 NRF为该消费者签发的、受众与 范围匹配且未过期的令牌，且令牌 主题与 TLS客户端证书身份一致。	无	成立	中	是
Z03	**受请求约束的主张。** 令牌的 主体、听觉、镜片、有效期与使用上下文逐项绑定；攻击者不能把某消费者的令牌用于另一消费者身份、另一 NWDAF 实例或 镜 外的操作。	无	成立	中	是
Z05	**消费者之间隔离的结果。** 在允许控制其他消费者域的前提下，目标消费者接受的通知只包含其自身订阅、自身 mlCorreId 的训练结果；其他消费者的结果与订阅不可见、不可错接。	无	不成立（1 个攻击）	中	否
S05	**终止后无通知。** 取消订阅成功或收到 termTrainReq 之后，NWDAF 不再为该订阅发送新通知；旧订阅标识不能重新获得通知权限。	无	成立	低	是
A04.10	**考虑每件接收件发送NWDAF份。** 消费者对同一通知实例至多接受一次，且每次接受都对应不同的 NWDAF 发送运行。	无	不成立（1 个攻击）	高	否
U01	**终止与结果不相容。** 消费者接受的通知中，termTrainReq 与 mLModelInfos/statusReport 的出现与 NWDAF 实际发送的字段一致，二者不可互相冒充。	无	不成立（1 个攻击）	高	否
Z05.12	**外国结果未被接受为自己的结果。** 在允许控制其他消费者域的前提下，目标消费者接受的通知只包含其自身订阅、自身 mlCorreId 的训练结果。	无	不成立（1 个攻击）	高	否

所问之问,及分析师之答:

问题	回答	依据
Q1: 已认证消息的重放是否仍满足规范允许的相关性语义	否:经认证的通知可以再次交付并再次接受,因为通知带有订阅的关联标识符,但没有实例或序列号。 使用相同相关性标识符的同名NF的两个订阅也被拼接,所以被接受的通知不能可靠地与它来自的发送连接起来.	A04, A04.10
Q2: 终止事件与普通结果的混淆是否由真实规范字段消除	仅部分:字段值将终止与结果区分开来,但API中没有任何内容将接收的字段与发送者联系起来,因此,知道回调的URI以及相关值的NF使得消费者接受从未发送的NWDAF的终止. 将经认证的发件人与其订阅的NWDAF进行对比的消费者,不可混淆.	U01, A02, D01
Q3: 不同消费者及训练任务之间结果隔离	保密性是:一个训练有素的模型只交付给被命名为notifUri的消费者,网络和另一个消费者都没有学习过. 隔离并不阻碍注射或订阅资源:另一个合法的NF可以将结果推向消费者的回调URI,一个知道subscriptionId的NF可以重写或取消订阅.	Z05, Z05.12, A03, A02

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:

- SBA型运输车型为公用密钥加密加签名,NF例身份为经认证的公用密钥; 3. TLS会场的建立,恢复,密码套件和证书链没有建模.
- 该令牌对发行者,主体,受众,范围和完整性进行验证,但对其到期时间则不进行验证:该型号没有时钟.
- 通知召回是模拟终点身份,而不是URI; 通知和订阅申请的重新定向答复(307、308)没有模式。
- 通过SCP或SEPP的间接通信,其中TS 33.501指出消费者和生产者之间没有相互认证,但这种通信没有模式化; 只有直接的SBA端点是.

- 消费者每订阅一次处理两次通知; 每项培训最多应提交两份状况报告,而审查国并不在来源单位,而且不是模拟的。
- mlCorreId和roundInd不是模拟检查; 消费者只将notifCorreId号通知与订阅有关,这是API号通知所述。
- PUT和PATCH是模拟更新行动; 未区分部分更新语义 。
- 删除是按订阅过程的寿命模拟的,而不是按表格模拟的,因此在DELETE之后已在飞行的通知不是模拟的; DELETE之后的重播通知仅通过重播结果覆盖.
- 训练有素的模型是按每个消费者一个价值而不是模型内容模拟的; 模型本身的正确性不在符号模型之外.
- 分析无法证明签名,信使或运输加密的计算安全性,也无法证明对量子攻击的阻力.
- 在一份模型(fix-sender)中检查了对通知发送人进行比较的建议。 页:1 关于增加通知序列号和资源一级授权号的建议没有在模型中加以检查。

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.

A02:经认证的请求和通知同行

每当 NWDAF 接受某消费者实例的订阅/更新/取消请求，或消费者接受 NWDAF 的通知，声称的对端必须确实以本方为对象运行过该协议。

消费者如果将一份通知的经认证的SBA00身份与其订阅的NWDAF实例进行比较,则只接受该实例发出的通知。 仅履行API规定的检查的消费者,即notifCorreId的平价,接受任何合法NF的通知,知道其召回URI和相关价值。

- 结果:失败(1次攻击); 回答问题:是的; 可用备注
- 价值高:它分离了同一API文本的两个读数,并显示API自己的支票没有认证通知; 文件没有说明这一后果。
- 在文件中说明:不明确。 资料来源:ts-33-501:2871、ts-33-501:2875、s0129、s0321、s0445。
- 休息时间:SBA的运输方式是仿照对接收器的公钥进行加密,外加发件人的签名,实例身份是认证的公钥. ; 两种消费行为是模拟的:一种是验证发货人,一种是只检查API州。 ; notifCorreId是作为攻击者可能知道的价值的模型,因为规格要求它不保密.
- 开放:消费者必须比较的NWDAF例ID是否在每次部署中都能得到(来自发现或订阅回复). ; 通知路径中的SCP是否改变消费者可以检查的内容.
- 下一步:通过SCP的模型间接通信,并询问攻击者下面的同一财产.

A03:通知和订阅关联

消费者接受通知时，须存在匹配的自身订阅运行，notifCorreId、notifUri、mlCorreId、roundInd 一致；NWDAF 接受更新/取消时，subscriptionId 须属于该消费者。

与notifCorreId持有的订阅通知相关:仅接受消费者自己的订阅价值. 订阅资源本身没有得到授权——代号授权服务,而不是资源——所以知道subscriptionId的NF号机可以删除或重写另一个消费者的订阅.

- 结果:失败(1次攻击); 回答问题:部分; 可用备注
- 价值高:资源级差距是文件未说明的规格的弱点; 攻击需要subscriptionId, 模型授予作为一个单独的攻击者。
- 在文件中说明:不明确。 资料来源: 492、s0378、s0442、s0105。
- 休息时间:NWDAF存储订阅的拥有者,并且不与其进行比较,因为规格定义了没有资源级的授权。 ; 密码subscriptionId被模拟为网络攻击者所不知道,并且被网络攻击者所知。sid_read攻击者。 ;PUT财务报告和财务报告PATCH模拟为一个更新操作。
- 打开: 执行是否添加所有者检查, 尽管 API 定义为无 。 ; subscriptionId数值在实践中如何猜测,这决定了sid_read攻击者是否现实.
- 下一步:PUT型机车,更改编号为notifUri,并询问外国通知是否随后到达sid_read型攻击机下的攻击者.

A04: 接受一次的每次通知活动

消费者对同一通知实例至多接受一次；若规范无序号字段，则须显式记录该性质不可由规范字段保证。

消费者不能从新的通知中分辨重复交付。 第二次接受从电线上取出并再次交付的通知,分得notifCorreId的同一NF的两笔订阅是无法区分的,因此接受另一笔通知。

- 结果:失败(1次攻击); 回答问题:是的; 可用
- 值高:它机械地显示,通知定义没有可以构建重播检查的字段,并且发现只有网络的攻击.
- 在文件中说明:否。 资料来源:s0129、s0321。
- 补充:每个发送器在模型中都得到一个新的实例标识符,没有指定字段提供; 输入式查询显示 API 所缺少的。 ; 消费者每次订阅都会处理两份通知,并且没有说明它已经接受什么。 ; notifCorreId是一个模拟的公共价值。
- 开放:每个订阅的部署的notifUri是否不同,这会限制拼写,而不是重播.
- 下一步:构建一个未滚动的消费者,保存最后接受的通知,并检查添加的序列号是否删除了重播.

D01:通知有效载荷完整性

消费者接受的每条通知，其发送方为订阅的 NWDAF，且 mLModelInfos、statusReport、termTrainReq 等载荷与 NWDAF 实际发送一致。

当消费者验证经认证的发送者时,其接受的每个机构——mLModelInfos、statusReport或termTrainReq——是其发送的NWDAF订阅机构。 当它只履行API的支票时,任何合法的NF都可以将自己选择的躯体放入消费者的回调URI.

- 结果:失败(1次攻击); 回答问题:是的; 可用备注
- 价值高:它表明通知的有效载荷完整性取决于API不需要的检查。
- 在文件中说明:不明确。 资料来源:ts-33-501:2875、s0128、s0131、s0133、s0137。
- 休息时间:交通作为公用密钥加密加签名,身份是认证的公用密钥. ; 描述的两种消费行为为A02.
- 开放:外地符合要求的消费者是否比较通知发送者; API不需要它,TS 33.501只要求一般的验证.
- 下一步:为验证有效载荷类型的消费者询问相同的属性,以对抗订阅的订阅事件.

K01:长期证书保密.

攻击者不能推导 NRF 的令牌签名私钥或任一 NF 的长期认证凭据。

NRF的标志性签名密钥和NF例的长期密钥都无法从网络上可见的任何东西中衍生出来,包括认证的公钥. 这是象征性原始人的财产,而不是关于其计算强度的声明.

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:直接源于原始物是声音的假设,分析不测试这种假设.
- 在文件中说明:是的。 文件上说:ts-33-501:2773,ts-33-501:2795,s0438,s0508
- 休息:没有密钥,签名和加密就假定是不可原谅和不可逆的.
- 打开:NRF的密钥管理是否将签名密钥保留在硬件中,而任务却忽略了这一点.
- 下一步:没有象征性模式; 关键管理层不在其中。

Z01:服务访问需要有效符号.

NWDAF 提交订阅/更新/取消操作时，须存在 NRF 为该消费者签发的、受众与 匹配且未过期的令牌，且令牌 subject 与 TLS 客户端证书身份一致。 7

订阅的每次创建、更新和删除都需要一个NRF-签名的代币,其发行商是NRF,其受众是NWDAF例,其范围是nwdaf-mlmodel训练服务。 没有这种标志的请求不会改变任何东西。

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:担保持有,但基于一个没有时间的模型; 过期检查是读者最希望覆盖的部分。
- 在文件中说明:是的。 其中文件主要有:338,ts-33-501:2867,s0375,s0507,s0515,s0518
- 信使是其债权的签字; 制作人用NRF公用密钥验证. ; 过期不是建模:一个符号值是建模为永久有效的.
- 打开:文件不支持吊销托肯,因此一个令牌在过期之前仍然可以使用; 该模型完全没有过期。
- 下一步:增加一个令牌过期和第二阶段,以询问一个存储的令牌在到期后是否仍然被接受.

Z03: 受请求约束的托肯主张

令牌的 主体、听觉、瞄准镜、有效期与使用上下文逐项绑定；攻击者不能把某消费者的令牌用于另一消费者身份、另一 NWDAF 实例或 瞄准镜、外的操作。

授权请求的令牌主体是经认证的TLS客户身份,因此发给一个NF个实例的令牌不能被另一个实例使用. 观众是这个NWDAF个案例,范围是服务名称,所以拒绝为另一个服务或另一个案例提供标志.

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:它以实际核对主张的模型复制了约束TS 33.501的主张要求。
- 在文件中说明:是的。 这些文件都说:ts-33-501:2795,ts-33-501:2801,s0483,s0513,s0515,s0518
- 休息:消费者身份为证书身份,仿照公用密钥. ; 一个单一的NWDAF例和单一的服务范围是模拟的.
- 开放:部署时是否使用NF型或NF套索偿要求; 模型将观众固定为一个实例。
- 下一步:模拟NRF套和两款NWDAF同型例,并询问一个观众的标志是否为另一个观众所接受.

Z05:在消费者之间隔离结果

在允许控制其他消费者域的前提下， 目标消费者接受的通知只包含其自身订阅、自身 mlCorreId 的训练结果； 其他消费者的结果与订阅不可见、不可错接。

一个训练有素的模型只触及到名为notifUri的消费者:另一个消费者和网络没有学习它. 消费者仍然接受一份自己订阅的通知,即另一个合法的NF生产,因此,内容的保密性在来源不受保护的情况下。

- 结果:失败(1次攻击); 回答问题:是的; 可用备注
- 值介质:它将保密的半部分与来源的半部分分开,后者没有,文件也没有说明通知行动。
- 在文件中说明:否。 资料来源:s0128、s0129、s0378。
- 休息时间:通知被封至以notifUri命名的终点. ; 训练有素的模型是以每个消费者一个价值为模式的。
- 打开: SCP或重定向是否改变通知的召回路径 。
- 下一步:在NWDAF型机车与消费者召回型机车之间搭建SCP型机车.

S05:终止后无通知.

取消订阅成功或收到 termTrainReq 之后， NWDAF 不再为该订阅发送新通知；旧订阅标识不能重新获得通知权限。

在模拟的生命周期中,通知只在订阅存在的情况下发出:NWDAF没有为它已经删除的订阅发送任何消息,而新的订阅总是得到新的标识。 证据取决于模型的修复顺序,而不是NWDAF的比较状态。

- 结果:持有; 回答问题:是的; 可用备注
- 值低:模型按顺序而不是按协议中的检查来修正属性,因此它只字未提文字。
- 在文件中说明:是的。 文中说:主:343,主:347,s0107,s0117,s0133

- 休息:订阅寿命是生产者的流程链,因此除去步骤后不存在通知步骤. ; 重新播放的通知在未订阅后仍可被消费者接受; 这是重播的结果, 这里没有覆盖。
- 开放: DELETE型飞机处理时已在飞行中的通知没有模拟; 是否在拆卸未打开后交付。
- 下一步:将DELETE型机型和未滚动生命周期中的飞行中通知型号模拟,并询问该通知是否仍然被接受.

A04.10: 区分 NWDAF 按接受发送

消费者对同一通知实例至多接受一次，且每次接受都对应不同的 NWDAF 发送运行。

接收不能与发送的一对一匹配,因为API没有给消费者任何识别通知实例的机会. ProVerif通过重播和两个共享相关标识的订阅,找到一个发送的两个接受.

- 结果:失败(1次攻击); 回答问题:是的; 可用
- 价值高:这是对通知定义所缺乏的准确的说明,通过追踪显示。
- 在文件中说明:否。 资料来源:s0129、s0321。
- 休息时间:该模型的新实例标识代表了API缺少的球场. ; 消费者没有接受通知的记录。
- 开放时间:与A04相同.
- 下一步:与A04相同:增加一个通知序列号,并在未滚动的生命周期中检查注射式查询.

U01:终止与结果不相容

消费者接受的通知中，termTrainReq 与 mLModelInfos/statusReport 的出现与 NWDAF 实际发送的字段一致，二者不可互相冒充。

通知机构对中间结果,完成和终止进行区分,对发件人进行验证的消费者不能将一种结果作为另一种结果。 仅检查相关标识的消费者接受NWDAF型机从未发送的终止通知,并停止等待其型号.

- 结果:失败(1次攻击); 回答问题:是的; 可用备注
- 价值高:它表明,终止信号是API最有害的通知,不受API要求的字段的约束。
- 在文件中说明:否。 资料来源:s0133、s0321、s0350。
- 休息时间:通知的种类是身体的一个领域,而不是一个单独的信息. ; 描述的两种消费行为为A02.
- 开放:消费者是否可以使用roundInd或mlCorreId通知伪造终止; 模型不检查它们。
- 下一步:将mlCorreId型机车作为消费者检查的价值,看看伪造的终止是否仍然在不知情的情况下被接受.

Z05.12: 不接受的外国结果为自己

在允许控制其他消费者域的前提下，目标消费者接受的通知只包含其自身订阅、自身 mlCorreId 的训练结果。

培训结果不向另一消费者或网络披露。 消费者接受另一个合法NF公司产生的结果,所以即使不能从电线上读出外国的结果也可以作为自己的结果提出.

- 结果:失败(1次攻击); 回答问题:是的; 可用备注
- 价值高:它陈述了API自身相关规则允许的隔离失败,文件没有提到这一点.
- 在文件中说明:否。 资料来源:s0129、s0135、s0321。
- 休息时间:通知封存到notifUri端点. ; 消费者只有notifCorreId人。
- 开放:部署的notifUri和notifCorreId是否每个订阅都是独一无二的,很难猜测,这决定了注射有多实用.
- 下一步:模拟一个可猜到的关联标识符,并单独在网络攻击者下询问相同的属性.

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
A02	proved		a02s	检查	a02l (holds_in_source)	证实1,1次攻击
A03	proved		a03a	检查	a03b (holds_in_source)	证实1,1次攻击
A04	无				a04 (holds_in_source)	1次攻击
D01	proved		a02s	检查	a02l (holds_in_source)	证实1,1次攻击
K01	proved		k01	检查		证明:1
Z01	proved		z01	检查		证明:3
Z03	proved		z01	检查		证明:2
Z05	proved		z05a	检查	a02l (holds_in_source)	证实1,1次攻击
S05	proved		s05	检查		证明:1
A04.10	无				a04 (holds_in_source)	1次攻击
U01	proved		a02s	检查	u01l (holds_in_source)	证实1,1次攻击
Z05.12	proved		z05a	检查	a02l (holds_in_source)	证实1,1次攻击

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
A02	消费者如果对其订阅的NWDAF实例(因为TS 33.501要求每NF次验证收到的电文)验证通知的运输身份,则只接受NWDAF实际发送的通知。	`network`	proved	a02s	检查
A02	通知检查API号本身规定——通知载有订货的notifCorreId号,并送交其notifUri号——验证发送者:进行这些检查的消费者只接受发送的NWDAF号通知。	`legit_nf`	攻击 (holds_in_source)	a02l(控制 a03a) (中文(简体)).	
A03	NWDAF只接受拥有subscriptionId号机车的消费者的更新或未订阅:URI号机车中命名的订阅属于请求的NF号机车.	`sid_read`	攻击 (holds_in_source)	a03b	
A03	接受的通知属于消费者自己创建的订阅:其notifCorreId等于消费者的订阅之一.	`network`	proved	a03a	检查
A04	消费者接受一次通知:每次接受均与NWDAF人发出的明确通知相对应。	`network`	攻击 (holds_in_source)	a04	
D01	消费者接受的每一份通知,包括其中的种类(中间结果、完成或终止),等于消费者按TS 33.501的要求对经认证的发送人进行验证时发出的订阅费NWDAF份通知的正文。	`network`	proved	a02s	检查
D01	一个只检查API国家支票的消费者接受通知机构——mLModelInfos、statusReport、termTrainReq——从它所订阅的合法的NF发送的NWDAF。	`legit_nf`	攻击 (holds_in_source)	a02l(控制 a03a) (中文(简体)).	
K01	NRF的代号签名密钥和NF例的长期密钥不能来自网络上的任何内容,甚至不能来自持有公用密钥的一方.	`network`	proved	k01	检查

目标	主张	攻击者	回答	查询	对照
Z01	NWDAF只为消费者开具NRF-签名的代币,其发行商为NRF,其受众为NWDAF例,范围为nwdaf-mlmodeltraining服务.	network	proved	z01	检查
Z01	密码NWDAF仅对提交NRF-与正确的发行者、受众和范围签署代号。	network	proved	z01u	检查
Z01	NWDAF号只取消了消费者的订阅费,该消费者出示了NRF-号署名的有正确发行者、受众和范围的代币。	network	proved	z01d	检查
Z03	授权请求的令牌的标的主张是请求人经认证的TLS客户身份,因此签发给一个NF例的令牌不能被另一个人使用.	network	proved	z01	检查
Z03	观众声称这是NWDAF例,范围主张是nwdaf-mlmodeltraining服务,用于授权订阅更新和删除的标语.	network	proved	z01u	检查
Z05	由于另一个消费者的领地在攻击者的控制下,目标消费者只接受自己订阅的通知和它订阅的NWDAF的通知.	legit_nf	攻击 (holds_in_source)	a02l(控制 a03a) (中文(简体)).	
Z05	消费者C订阅的训练有素的模型不向其他方披露:携带该模型的通知被封存到命名为notifUri的端点,因此网络和另外的NF都没有学习模型值.	network	proved	z05a	检查
S05	通知只在NWDAF人创建并仍在持有的订阅书内发出; 订阅被删除后,将不发送任何信息 。	network	proved	s05	检查
A04.10	每一份通知的接受均相当于NWDAF号通知发出的一份单独通知; 同一寄件者从未接受过两次。	network	攻击 (holds_in_source)	a04	
U01	当消费者对经认证的发送者进行验证时,每一份被接受的通知(包括终止培训,termTrainReq)的种类等于发送的NWDAF的通知书的种类,因此无法得出终止或相反的结果。	network	proved	a02s	检查
U01	仅检查API的消费者表示接受NWDAF从未发出的终止通知(termTrainReq)。	legit_nf	攻击 (holds_in_source)	u01l(控制 a02s) (中文(简体)).	
Z05.12	目标消费者不接受另一个消费者的培训结果,也不接受另一个ML程序的培训结果。	legit_nf	攻击 (holds_in_source)	a02l(控制 a03a) (中文(简体)).	
Z05.12	消费者C订阅的训练结果不向另一消费者或网络透露,因此无法从电线上接管.	network	proved	z05a	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-20261114T235758, 2026-11-14. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:70,校对:76 s,壁21 min,耗资0.192 USD.

ProVerif:112 证明运行,110 决定,2 未答,53 s,31 答录.

分析了什么

协议	审查经认证的训练活动
版本	19.8.0
分析范围	复核首轮 MLModelTraining 事件订阅/更新/通知/取消，真实 SBA 端点认证与密钥隔离；最多两次训练状态报告，显式区分中间结果、完成、失败和取消；无通知序号时不能发明序号并归功于规范，不以单调表假装删除。
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694个编号段落(323317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	4.6	Nnwdaf_MLModelTraining 服务
主体	4.6.1	服务说明
主体	4.6.1.1	概览
主体	4.6.1.2	服务架构
主体	4.6.1.3	网络函数
主体	4.6.1.3.1	网络数据分析函数(NWDAF)
主体	4.6.1.3.2	NF 服务消费者
主体	4.6.2	服务业务
主体	4.6.2.1	导言
主体	4.6.2.2	Nnwdaf_MLModelTraining_Subscribe次服务业务
主体	4.6.2.2.1	A. 概况
主体	4.6.2.2.2	事件通知的订阅
主体	4.6.2.2.3	更新事件通知的订阅
主体	4.6.2.2.4	事件通知的部分更新订阅
主体	4.6.2.3	Nnwdaf_MLModelTraining_Unsubscribe次服务业务
主体	4.6.2.3.1	A. 概况

文稿	章节	标题
主体	4.6.2.3.2	从事件通知中取消订阅
主体	4.6.2.3.3	从事件通知中取消订阅,提供更多信息
主体	4.6.2.4	Nnwdaf_MLModelTraining_Notify次服务业务
主体	4.6.2.4.1	A. 概况
主体	4.6.2.4.2	关于订阅活动的通知
主体	5.5	Nnwdaf_MLModelTraining服务 API
主体	5.5.1	导言
主体	5.5.2	使用费HTTP美元
主体	5.5.2.1	A. 概况
主体	5.5.2.2	HTTP标准标题
主体	5.5.2.2.1	A. 概况
主体	5.5.2.2.2	内容类型
主体	5.5.2.3	HTTP 个自定义标题
主体	5.5.3	资源
主体	5.5.3.1	资源结构
主体	5.5.3.2	资源:NWDAF ML 示范培训订阅
主体	5.5.3.2.1	说明
主体	5.5.3.2.2	资源定义
主体	5.5.3.2.3	资源标准方法
主体	5.5.3.2.3.1	POST
主体	5.5.3.2.4	资源自定义操作
主体	5.5.3.3	资源:个人 NWDAF ML 示范培训订阅
主体	5.5.3.3.1	说明
主体	5.5.3.3.2	资源定义
主体	5.5.3.3.3	资源标准方法
主体	5.5.3.3.3.1	PUT
主体	5.5.3.3.3.2	PATCH
主体	5.5.3.3.3.3	DELETE
主体	5.5.3.3.4	资源自定义操作
主体	5.5.3.3.4.1	概览
主体	5.5.3.3.4.2	操作: 未订阅 - info
主体	5.5.3.3.4.2.1	说明
主体	5.5.3.3.4.2.2	操作定义
主体	5.5.4	没有相关资源的自定义操作
主体	5.5.5	通知
主体	5.5.5.1	A. 概况

文稿	章节	标题
主体	5.5.5.2	事件通知
主体	5.5.5.2.1	说明
主体	5.5.5.2.2	操作定义
主体	5.5.6	数据模型
主体	5.5.6.1	A. 概况
主体	5.5.6.2	结构化数据类型
主体	5.5.6.2.1	导言
主体	5.5.6.2.2	NwdafMLModelTrainSubsc型机车
主体	5.5.6.2.3	NwdafMLModelTrainSubscPatch型机车
主体	5.5.6.2.4	虚拟
主体	5.5.6.2.5	MLModelTrainInfo型机车
主体	5.5.6.2.6	MLTrainReportInfo型机车
主体	5.5.6.2.7	FailureEventInfoForMLModelTrain型机车
主体	5.5.6.2.8	NwdafMLModelTrainNotif型机车
主体	5.5.6.2.9	虚拟
主体	5.5.6.2.10	DataAvReq型机车
主体	5.5.6.2.11	DelayEventNotif型机车
主体	5.5.6.2.12	StatusReportInfo型机车
主体	5.5.6.2.13	TrainDataInfo型机车
主体	5.5.6.2.14	TrainingUnsubscribeInfo型机车
主体	5.5.6.3	简单数据类型和计数
主体	5.5.6.3.1	导言
主体	5.5.6.3.2	简单数据类型
主体	5.5.6.3.3	编号: FailureCodeTrain
主体	5.5.6.3.4	编号: TermTrainCause
主体	5.5.6.3.5	编号: DelayCause
主体	5.5.6.3.6	编号: FLServerTermCause
主体	5.5.7	处理错误
主体	5.5.7.1	A. 概况
主体	5.5.7.2	协议错误
主体	5.5.7.3	应用程序错误
主体	5.5.8	特性谈判
主体	5.5.9	警卫
ts-33-501	13.4	授权NF次服务访问
ts-33-501	13.4.1	OAuth 2.0 网络功能服务访问授权
ts-33-501	13.4.1.0	A. 概况

文稿	章节	标题
ts-33-501	13.4.1.1	PLMN范围内的服务准入授权
ts-33-501	13.4.1.1.1	OAuth 2.0 角色
ts-33-501	13.4.1.1.2	服务请求进程
ts-33-501	13.4.1.1.3	部署中访问令牌请求数NRFs
ts-33-501	13.4.1.1A	互联情况下的服务访问授权
ts-33-501	13.4.1.2	在漫游情况下的服务访问授权
ts-33-501	13.4.1.2.1	OAuth 2.0 角色
ts-33-501	13.4.1.2.2	服务请求进程
ts-33-501	13.4.1.3	间接通信情况下的服务访问授权
ts-33-501	13.4.1.3.1	授权不经授权的发现程序进行间接通信
ts-33-501	13.4.1.3.1.1	在运输层的NF和服务消费者与NRF之间相互认证
ts-33-501	13.4.1.3.1.2	运输层NF至NRF之间没有相互认证
ts-33-501	13.4.1.3.2	授权与授权的发现程序进行间接通信
ts-33-501	13.4.1.4	NF人之间流动情况下的服务准入授权
ts-33-501	13.4.1.5	与间接通信连接和漫游情况下的服务访问授权
ts-33-501	13.4.1.5.1	A. 概况
ts-33-501	13.4.1.5.2	授权在源网络中选择 NF
ts-33-501	13.4.1.5.2.1	A. 概况
ts-33-501	13.4.1.5.2.2	授权与授权的发现程序进行间接通信或没有授权的发现程序
ts-33-501	13.4.1.5.3	授权在目标网络中选择 NF
ts-33-501	13.4.1.5.3.1	A. 概况
ts-33-501	13.4.1.5.3.2	授权不经授权的发现程序进行间接通信
ts-33-501	13.4.1.5.3.3	授权与授权的发现程序进行间接通信

协议的目的是在文档中将其定位为源步骤:复核首轮 MLModelTraining事件订阅/更新/通知/取消，真实 SBA 端点认证与密钥隔离；最多两次训练状态报告，显式区分中间结果、完成、失败和取消；无通知序号时不能发明序号并归功于规范，不以单调表假装删除。

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
A02	请求和通知的认证同行	密码NWDAF包含MTLF请放心,订阅/更新/未订阅请求已由 NF(a) 在运输层验证其实例; 编号NF向服务消费者保证,它处理的通知来自:NWDAF它同意这样做。	TS 33.501 需要在NF 服务消费者和 NF 服务生产者之间进行相互认证, 以便进行直接通信,每NF 个用户必须验证收到的电文; 通知是给消费者的notifUri的POST,没有OAuth的保护。	ts-33-501:2871,ts-33-501:2875,主场:344,s0128,s0138,s0505,s0522

ID	简称	对象	文稿怎么说	出处
A03	通知和订阅关系	消费者只接受它创建的订阅通知(notifCorreId、notifUri、mlCorreId、roundInd一致); NWDAF仅对拥有subscriptionId的消费者接受更新或未订阅。	notifCorreId的数值应与订阅时的数值相同; 通知送交订阅的notifUri; 第API号决议只界定了整个服务范围,没有资源范围,因此资源所有权不是象征性的。	主机:351,主机:347,主机:492,s0037,s0042,s0129,s0321,s0378
A04	接受一次的每次通知事件	NF服务消费者接受每NWDAF次发送一次通知; 该规格未定义通知序列号,只有notifCorreId。	NwdafMLModelTrainNotif载有notifCorreId,没有通知序列或实例识别符; 文件上没有关于重播通知的内容。	s0129, s0321
D01	通知有效载荷完整性	消费者接受的每份通知均由订户NWDAF人发出,发送内容与mLModelInfos,statusReport和termTrainReq相同,发送内容为NWDAF.	消费者在收到通知时储存通知; OAuth2没有涵盖通知操作,文件要求消费者不检查有效载荷来源。	主机:349,ts-33-501:2807,s0128,s0131,s0133,s0137,s0138
K01	长期证书保密	NRF的存取式签名密钥和NF例的长期认证证书都保存在对方手中.	访问令牌是JWS-保护与保护NRF键,制片人用NRF公用密钥;NF全权证书持有人必须保密。	ts-33-501:2773,主机:340,s0438,s0508,s0375
Z01	服务访问需要有效的符号	NWDAF只当消费者出示了NRF-签名的访问信使,其发行人,受众和范围与这一NF服务相匹配时,才接受订阅,更新或不订阅.	Nnwdaf_MLModelTraining API号机的接入可能以OAuth2号机获得授权,NRF号机为授权服务器,由制作方核查该信使的签发者,签名,受众和范围.	主机:338,ts-33-501:2867,s0375,s0507,s0515,s0518
Z03	受请求约束的托肯主张	信使主题与经认证的TLS客户案例,这NWDAF个案例的观众以及这一服务的范围联系在一起,因此,为一个消费者发行的信使不能被另一个消费者使用,也不能被另一个服务使用.	制作方检查主体主张是否符合TLS客户证中的NF例ID,观众是否与自己身份相符,范围是否与请求的服务业务相符.	ts-33-501:2795, ts-33-501:2801, s0483, s0513, s0515, s0518
Z05	消费者之间隔离的结果	由于另一个消费者领域在攻击者控制下,目标消费者的通知只携带自己的订阅和自己的训练结果,其他消费者的结果也不向它透露.	该通知送交订阅的notifUri人,并载有该订阅的notifCorreId和mlCorreId; API号定义了没有资源级范围,因此隔离取决于关联性和运输特性.	主机:492,主机:349,s0027,s0128,s0129,s0135
S05	终止后无通知	在NWDAF取消订阅后,或要求以termTrainReq终止培训后,不再发出订阅通知,无法再次使用标识符进行新的订阅.	DELETE成功时,NWDAF取消了相应的订阅; termTrainReq表示将不再提供有关订阅的通知。	主机:343,主机:347,s0107,s0117,s0133
A04.10	按接受情况发送NWDAF份通知	消费者对通知的每次接受均相当于NWDAF号通知的单独发送; 同一寄件者从未接受过两次。	通知结构中没有任何序列号或实例标识,使消费者能够从新的序列号或实例中得知一次重复交付; 这些文件没有说明它。	s0129, s0321
U01	终止与结果不相容	消费者接受为培训终止的通知(termTrainReq)于NWDAF号作为终止通知发出; 不得以结果或状况报告作为终止或相反的理由。	delayEventNotif,mLModelInfos或termTrainReq中至少应有一个存在,其中一些是相互排斥的,但没有任何东西将接收的球场与发送方联系在一起.	主机:346、s0133、s0137、s0321、s0350

ID	简称	对象	文稿怎么说	出处
Z05.12	不接受的外国结果	目标消费者在攻击者控制下拥有另一个消费者领域,因此不接受另一个消费者或另一个ML程序的训练结果作为自己的.	该通知载有订户的notifCorreId份和可选择的mlCorreId份; 消费者仅以notifCorreId通知其订阅。	主机:351,s0129,s0135,s0321

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 28 段，没选 370 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	安全考虑的介绍性案文; 它没有说明它自己的要求。
P003 至 P006	rfc6749:2790-2823	Z01, Z03	
P007 至 P008	rfc6749:2827-2838	A02, Z03, `legit_nf`	
P009 至 P010	rfc6749:2840-2850	不在范围内	资源所有人认证和重复授权请求属于授权代码授权; API使用没有资源拥有者的客户证书。
P011 至 P015	rfc6749:2859-2881	Z03, K01	
P016 至 P021	rfc6749:2885-2917	不在范围内	刷新符不是NF服务访问所使用的客户证书授权的一部分.
P022 至 P025	rfc6749:2921-2943	不在范围内	授权代码不为客户证书授权所使用。
P026 至 P029	rfc6749:2947-2980	不在范围内	调整授权代码赠款的URIs; NF通知 URI是订阅属性,由A03和Z05处理.
P030 至 P033	rfc6749:2984-3003	不在范围内	不使用资源所有人密码证书。
P034 至 P035	rfc6749:3013-3019	K01, Z05, `network`	
P036	rfc6749:3023-3028	A02, Z01, `network`	
P037 至 P039	rfc6749:3032-3041	K01, `network`	
P040 至 P042	rfc6749:3045-3066	不在范围内	对终端用户的欺骗; 没有最终用户参与NF服务访问.
P043 至 P048	rfc6749:3070-3110	不在范围内	跨站点请求伪造需要基于浏览器的客户端和用户证书; 4.SBAA. 请求的提出者NFs超越彼此TLS.
P049 至 P050	rfc6749:3119-3138	不在范围内	点击劫持涉及用户代理渲染; 此协议中没有用户代理 。
P051 至 P052	rfc6749:3142-3150	证明器问不了	针对代码注入的输入验证力强,是象征式协议模型无法表达的一种执行属性.

段落	出处	定为	不选的原因
P053 至 P054	rfc6749:3154-3167	不在范围内	在浏览器流中打开重定向器; SBA请求的重定向是运营商网络内部的3xx响应,而不是模拟.
P055 至 P062	rfc6749:3170-3210	不在范围内	隐性赠款及其使用权滥用不适用于客户证书的发放。
P063	ts-33-501:2491-2491	不在范围内	任务排除了安全算法的竞价下调:分析不建模算法谈判或计算强度.
P064 至 P072	ts-33-501:2495-2511	不在范围内	UE与网络(SUPI认证,服务网络授权)之间的认证与授权——任务涵盖Nnwdaf_MLModelTraining API子程序,而非5G访问认证.
P073 至 P074	ts-33-501:2515-2517	不在范围内	5GC和NG-RAN的关键要求,在SBI API子程序之外.
P075 至 P125	ts-33-501:2523-2631	不在范围内	用户数据和信号数据保密性、完整性和用户隐私超过NAS/AS和UDM/UDR; 不是NF服务 API在这里检查。
P126 至 P198	ts-33-501:2637-2811	不在范围内	gNB、ng-eNB、SEAF、AMF和接入网络信号保护所需经费; 在SBI API次程序之外.
P199 至 P213	ts-33-501:2819-2853	不在范围内	订户对SEPP、UDM和SIDF的隐私要求; 不是这里检查的NF服务 API
P214	ts-33-501:2859-2859	没有陈述目标	它描述了5G系统的信任界限,并强加了任何可以攻击的要求.
P215	ts-33-501:2865-2865	Z01, A04, `network`	
P216	ts-33-501:2867-2867	Z01, `network`	
P217	ts-33-501:2869-2869	不在范围内	在行政领域之间隐藏的地形学涉及基于SEPP-的域间通信,这不属于这个直接的SBA子程序.
P218	ts-33-501:2871-2871	A02, `network`, `legit_nf`	
P219	ts-33-501:2873-2873	不在范围内	NOTE涉及通过SCP或SEPP进行间接通信,没有相互认证; 任务模型仅直接指向SBA端点.
P220	ts-33-501:2875-2875	A02, D01, U01, `legit_nf`	
P221 至 P227	ts-33-501:2879-2891	Z01, Z03, `network`	
P228 至 P241	ts-33-501:2895-2923	不在范围内	NEF和SCP的安全要求涉及接触和间接通信,而不是本文分析的直接Nnwdaf_MLModelTraining访问.

段落	出处	定为	不选的原因
P242 至 P292	ts-33-501:2929-3031	不在范围内	总体安全,SEPP和漫游的互联要求; 任务不包括漫游和互联。
P293 至 P314	ts-33-501:3035-3081	不在范围内	由漫游中间人生成的信息,保护超过N32和IPUPS的属性; 在直接的SBA子程序之外.
P315 至 P318	ts-33-501:3085-3091	不在范围内	3gpp-Sbi-Originating-Network-Id头条服务于PLMN路由之间; 漫游和网络识别器都在本分析之外.
P319 至 P337	ts-33-501:3097-3141	不在范围内	信号监测和安全可见度/配置涉及操作员程序,而不是协议信息。
P338 至 P369	ts-33-501:3149-3215	不在范围内	加密与完整性算法标识符和算法选择:任务排除了原始和算法谈判的计算强度.
P370 至 P396	ts-33-501:3219-11443	不在范围内	5G-RG、NSSAAF、N3、EAP-TLS出入、IAB和MBS所需经费; 没有一个涉及Nnwdaf_MLModelTraining API次程序.
P397 至 P398	ts-33-501:11899-11901	不在范围内	NEF-00项具体要求,约UE项识别资料和VFL项通信; NEF号不是这个API次程序的一部分。

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 25 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 6 项，没设的 19 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	`legit_nf`	
S02	NWDAF	参与方	按定义全部失守	随着NWDAF本身在攻击者控制之下,它发送的每一份通知都由攻击者发出,因此关于生产者诚实的属性被定义为丢失了; 这些文件没有要求这 API 的其他财产 在一个不诚实的生产者。
S03	NRF	参与方	按定义全部失守	在攻击者手中拥有授权服务器及其签名密钥时,每一个象征性的声称都可以被铸造出来; 分析没有要求这API 的财产 在一个妥协的NRF。
S04	消费者 A	参与方	按定义全部失守	消费者A是自认和结果为资产的一方; 如果甲本身不诚实,则甲所剩无几,是无法保证的。
S05	消费者 B	参与方	`legit_nf`	
S06	NF 实例身份	值	攻击者得不到更多	NF个实例身份是证书和标志的主体; 它通过建筑是公开的,持有它不会增加任何超出网络的范围。
S07	订阅资源	值	`sid_read`	
S08	notifCorreId	值	攻击者得不到更多	notifCorreId是由消费者自己选择的,每份订阅通知中都有回响,不需要规格保密.
S09	notifUri	值	攻击者得不到更多	notifUri是消费者自己的召回地址,公布后,NWDAF号可以到达; 2. 明知其不允许缔约方阅读封存到消费者端点的通知。
S10	mlCorreId	值	攻击者得不到更多	mlCorreId名称ML程序、订阅和联邦学习通知; 它是一个识别器,而不是一个证书。

ID	参与方或值	类别	攻击者条件	不设的原因
S11	roundInd	值	攻击者得不到更多	roundInd是一个圆形计数器,安装在订阅和通知内。
S12	subscriptionId	值	`sid_read`	
S13	通知实例	值	攻击者得不到更多	该规格定义了完全没有通知实例标识符,因此缔约方没有这种价值可持有; 该模型只引入一个来说明财产。
S14	mLModelInfos	值	攻击者得不到更多	mLModelInfos是通知的有效载荷,密封在消费者的端点; 2. 持有武器恰恰是Z05所保护的资产,不是攻击者的能力。
S15	statusReport	值	攻击者得不到更多	statusReport是通知有效载荷的一部分,密封在消费者的端口.
S16	termTrainReq	值	攻击者得不到更多	termTrainReq是通知有效载荷的一部分,密封在消费者的端口.
S17	delayEventNotif	值	攻击者得不到更多	delayEventNotif是通知有效载荷的一部分,密封在消费者的端口.
S18	NRF 令牌签名私钥	值	按定义全部失守	如果攻击者持有NRF的签名密钥,那么每个信物都是可伪造的,而且这API的每一个授权财产按照定义都会丢失; 这就是K01失败的意思, 不是文件给其他目标的攻击者。
S19	NF 长期认证凭据	值	`legit_nf`	
S20	访问令牌	值	攻击者得不到更多	(a) 进入信使被封存到其为消费者签发的终点; 另一方不能阅读它,一个人自己的身份的象征就是legit_nf已经拥有的东西.
S21	范围	值	攻击者得不到更多	这个API的范围是一个单一的公共服务名称,nwdaf-mlmodeltraining.
S22	观众	值	攻击者得不到更多	观众是NWDAF案例的公开身份,公布于NF简介.
S23	过期	值	攻击者得不到更多	到期时间是该纪念物的公开权利要求; 模型不建模时间,而持有过期值则无济于事。
S24	主题	值	攻击者得不到更多	主体是消费者的公众NF例身份.
S25	订阅状态	值	`sid_read`	

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		
`legit_nf`	一个恶意但合法的NF服务消费者:它自己的长期TLS密钥配对和访问令牌将NRF号的发行权赋予它自己的亲身身份,因此它可以打开SBA号与任何端点的连接,并以自己的身份发出请求. 它没有另外NF的密钥或标志.	TS 33.501要求消费者和生产者相互认证,并规定OAuth2框架必须适用于NF服务; 因此,登记在册的NF持有自己的证书和证物,而且文件中没有任何内容阻止登记在册的NF成为恶意行为。	ts-33-501:2889, ts-33-501:2873, s0438, s0505
`sid_read`	legit_nf型攻击机加上另一个消费者订阅的subscriptionId型,从该型NWDAF型存储订阅资源或信号监测机上读取.	subscriptionId是PUT/PATCH/DELETE中命名订阅资源的唯一价值,API界定了整个服务范围,没有资源一级的授权,因此所有权取决于是否知道标识; 文件允许对5GC信号进行NF监测。	ts-33-501:3097,主机:492,s0105,s0378,s0442

ID	`network`	`legit_nf`	`sid_read`
A02	成立	不成立	

ID	network	legit_nf	sid_read
A03	成立		不成立
A04	不成立		
D01	成立	不成立	
K01	成立		
Z01	成立		
Z03	成立		
Z05	成立	不成立	
S05	成立		
A04.10	不成立		
U01	成立	不成立	
Z05.12	成立	不成立	

关于证明和模型的说明

分析师给目标取了什么名字?

步骤	目标	特性	原因：
53	A02, A03, A04, D01, K01, Z01, Z03, Z05, S05, A04.10, U01, Z05.12	plain_primitives, many_sessions	该型号仅使用签名和公钥加密(SBA运输)作为普通原始,外加NRF的签名代币; 没有其他的代数定律 要求属性为任何数量的消费者和生产者会话,任何目标都不取决于一方所保存和更改的计数器或序列号——通知中缺少这样的值正是重播结果所显示的.

分析员的结语

所有12个目标都被按要求回答,有控制,并抽取了流量和9个攻击数字. 已证实的任何会议次数:服务准入和每次订阅变更都需要NRF-个签名的标志,其发行人、受众、范围和对象(受TLS客户身份约束)都得到检查(Z01、Z03、K01); 验证经认证的发件人的消费者只接受NWDAF发出的通知及其发送的体型(A02、D01、U01); 一个训练有素的型号只透露给名为notifUri(Z05,Z05.12)的消费者; 通知只在订户内发出,该订户为NWDAF人(S05人); 接受的通知载有消费者自己认购的notifCorreId(A03)。 袭击,所有holds_in_source:一名API-升的消费者接受一名合法的NF(A02、D01、U01、Z05、Z05.12)伪造的通知; 复播时再次接受通知,共享notifCorreId的两次订阅被拼接,因为通知没有实例编号(A04, A04.10); 任何NF带有服务标志,受害者subscriptionId可以删除或重写订阅,因为API授权服务而非资源(A03,攻击者sid_read). 3项调查结果,2项高,1项新颖性不明,因为主文:492规定了单一范围规则,但没有造成后果; 在一份模型上检查了发送方-比较方的建议。 封存更多:令牌过期、DELETE之后的飞行通知和增加的序列号需要未滚动的生命周期和时间(Tamarin+ Agent); 通过SCP的间接通信在模型之外.