对NWDAF个用户用户转账控制进行安全分析

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))
检查的性质	11 条：7 条成立，4 条不成立（7 个攻击）
发现	1

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

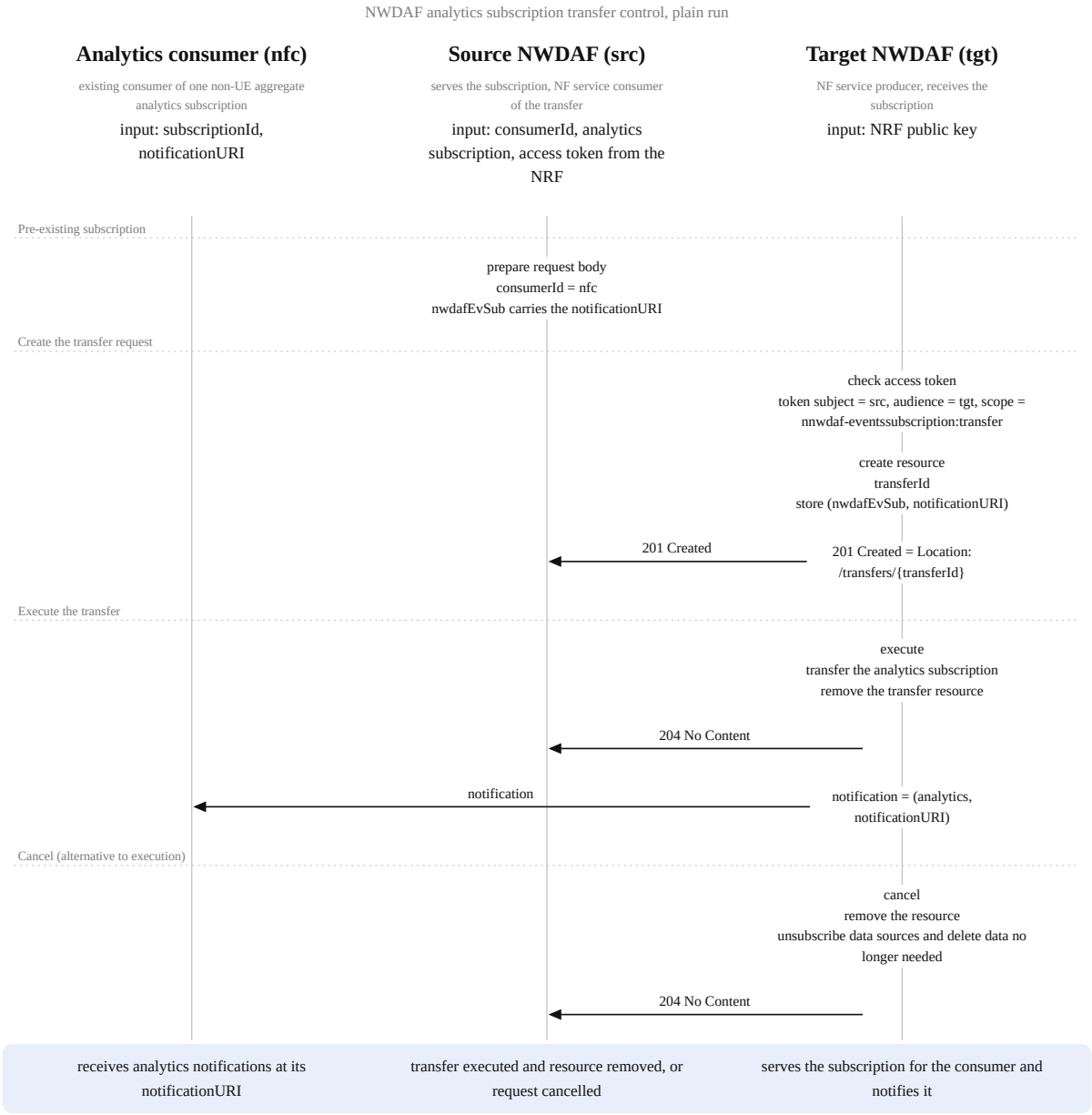
Nnwdaf_EventsSubscription_Transfer次服务业务允许NWDAF次案例向另外NWDAF次案例提供现有的分析订阅。 3个缔约方参加:现有的分析消费者nfc,持有1个非UE的总分析订阅和它想要通知的notificationURI; 来源NWDAF src ,为该用户服务,并担任转账的NF服务消费者; 以及接收订阅的NWDAF tgt的目标.

来文方以POST和PREPARE号机体提出转移请求,以transferId号机体收到201号机体,以PUT号机体和TRANSFER号机体执行,目标随后向消费者发出分析通知. DELETE号协议取消了一项准备中的请求。 每项请求均载有从NRF号机上获得的OAuth2号进入信使; notificationURI在nwdafEvSub和consumerId的旅游中 将分析师的消费者命名为分析师。

双方:

- **分析消费者(nfc)**:一个非UE的总分析用户的现有消费者。 持有量:subscriptionId,notificationURI.
- **来源:NWDAF(src)**:服务于订阅者,NF 服务用户转帐. 持有:consumerId,分析订阅,NRF号机车的存取信使.
- **目标NWDAF(tgt)**:NF 服务生产者,接受订阅. 持有:NRF公用密钥.

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

分析得出了1项结论:以下内容没有在文件中说明。 对于其中的1人,不清楚文件是否说明了这一点。

协议没有给出它打算给予的财产:一个合法的NF持有自己的有效转录镜代币可以使目标NWDAF接受和执行一个指定另一个消费者订阅的转录,这样消费者的notificationURI就可以被攻击者所取代. 这是唯一的发现; 文件只一般性地警告说,服务级别的范围不得允许不当的书写访问,而且不得说明失败。 仅针对网络,协议行为正确:无法更改字段,与源控件,符号检查控件达成协议,传输资源拒绝重播和重传. 在这11个目标中,有7个得到证实或有管制的核查,有4个有携带的攻击; 每一个答案都基于列出为极限的模型简化.

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.

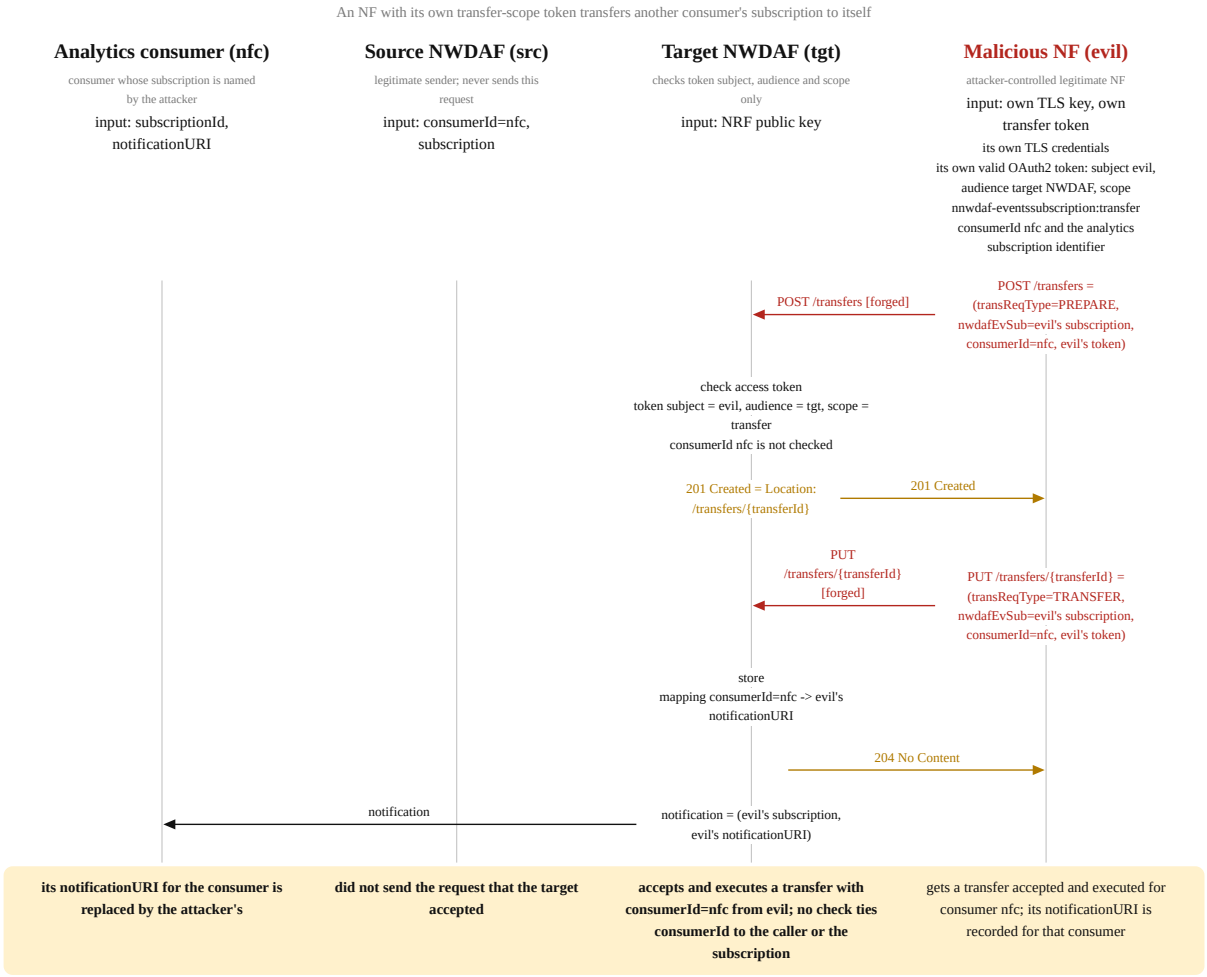
2.1 一个合法的NF可以将另一个消费者的分析订阅权转让给自己

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 (ts-29-501:1801, ts-33-501:8040)
价值	高
涉及的性质	A03, Z03, Z03.10, A03.8 （见第 3 节）
原文	s0014, s0020, s0022, s0152, s0184
依据	ProVerif 攻击询问 `z0310_nfc`,`z03b`,`a038_nfc`; 图2、3、4和5

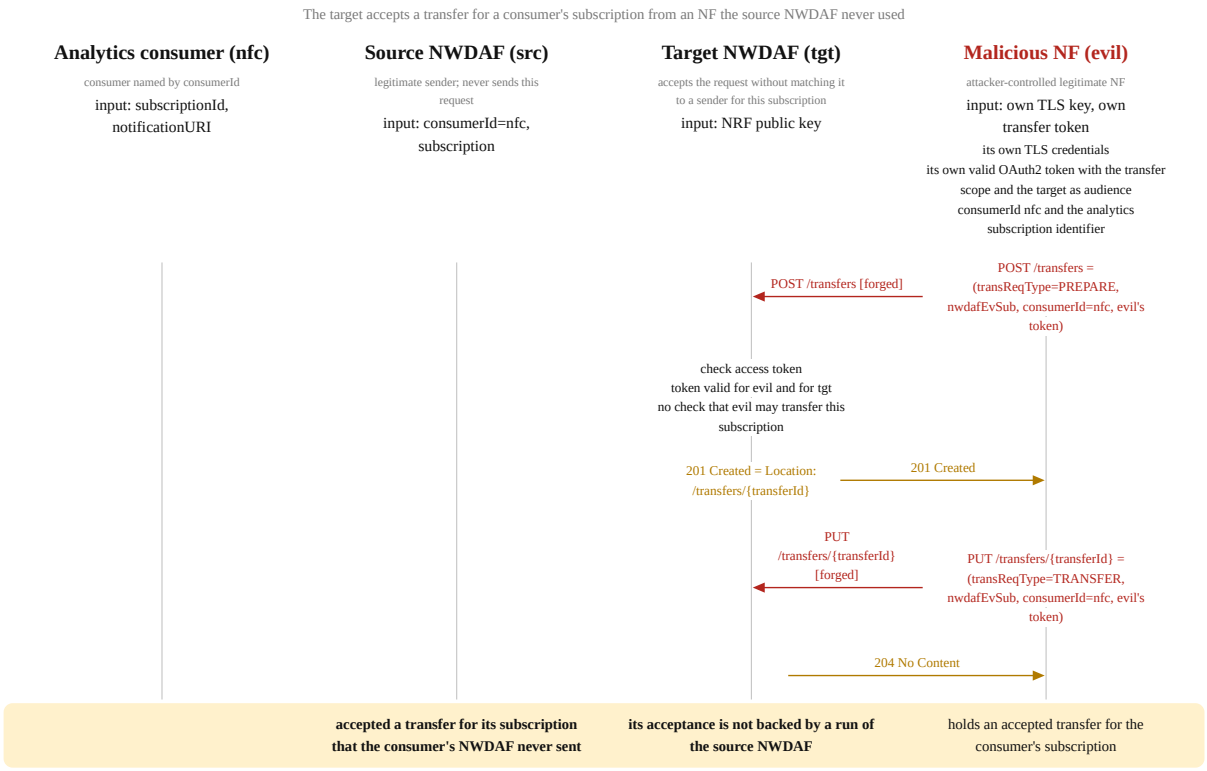
发生了什么。 目标NWDAF请检查access-date=中的日期值 (帮助) 请检查access-date=中的日期值 (帮助) Access-date=中的日期值 (帮助) Access-date=中的日期值 (帮助) Access-date=中的日期值 (帮助) Access-date=中的日期值 (帮助) Access-date=中的日期值 (帮助) Access-date=中的日期值 一个合法的NF实例,以显示它自己的有效转移范围符号,因此得到接受的转移请求。consumerId设定给另一个消费者, 创建传输资源, 执行它, 并有目标记录自己的notificationURI给那个消费者 来源NWDAF从来没有发出过请求。

攻击者需要什么。 攻击者是合法的。NF实例与它自己的TLS全权证书及其有效证明OAuth2nwdaf- events 订阅的访问令牌: 带有目标的传输范围NWDAF作为观众。 它需要的就是... . . . .consumerId目标消费者和分析的订阅标识符,两者均包含在nwdafEvSub/consumerId在基于服务的界面上。

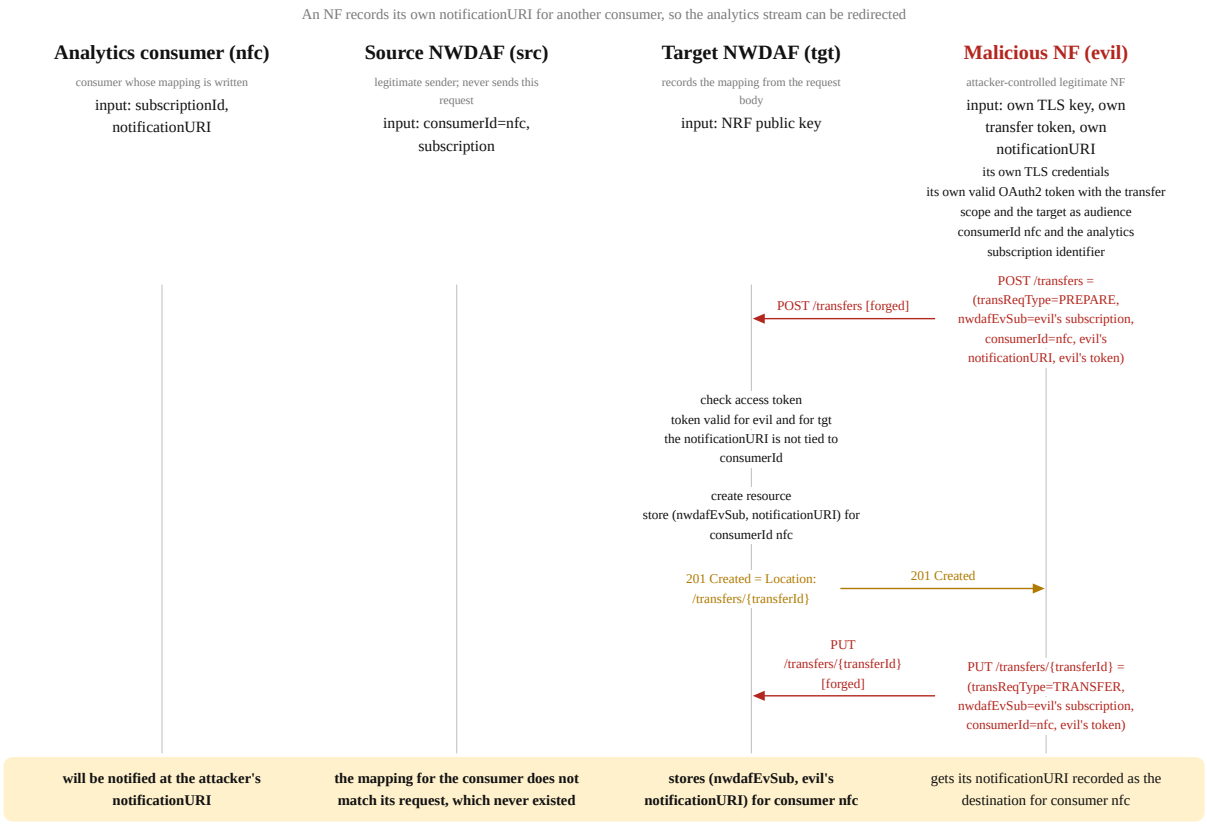
攻击者能得到什么。 攻击者可以为另一消费者的订阅创建和执行转帐,因此目标将消费者与攻击者notificationURI有关联; 之后的消费者分析通知可以直接给攻击者,消费者失去其分析流.



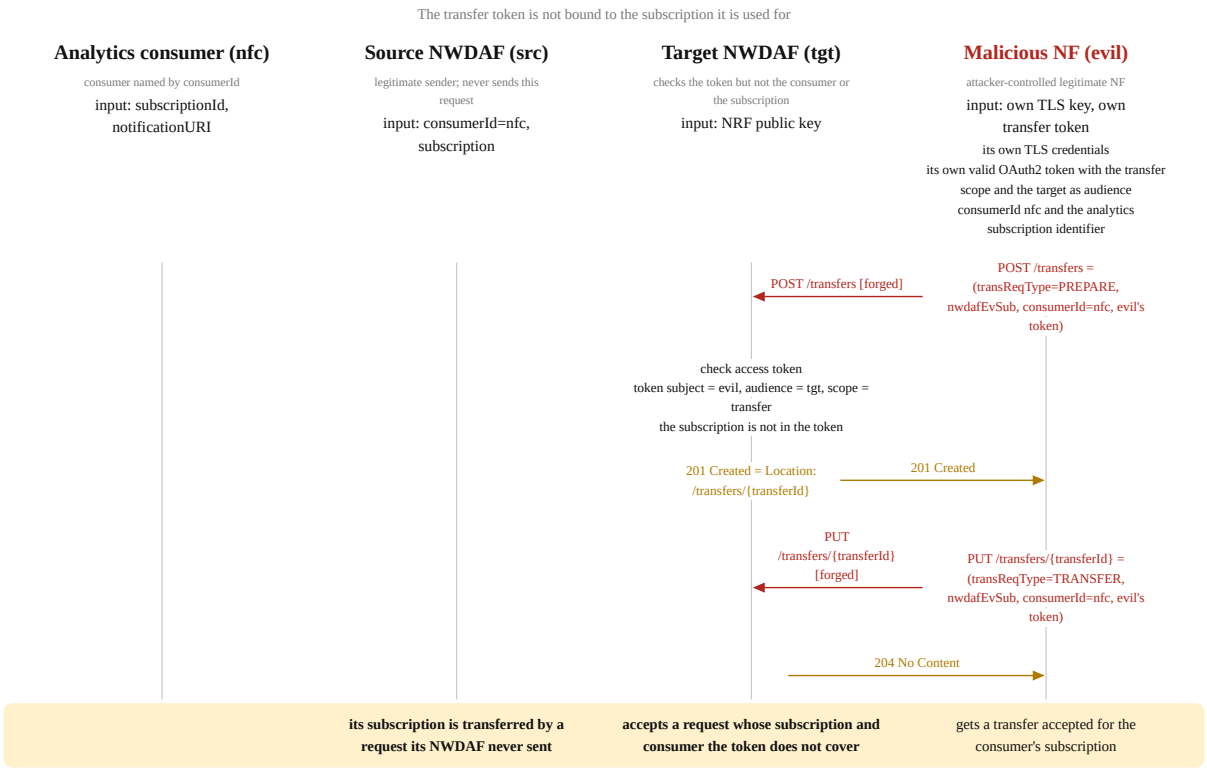
- 图2。 装有自身传动镜标志的NF号机将另一个消费者的订阅权转让给自己. 财产Z03.10; z0310,z0310_nfc攻击询问。 *



- 图3。 目标接受从NF的消费者订阅费转帐,而NWDAF的来源从未使用。 财产A03; a03_any z03b 攻击询问。 *



- 图4。 NF型机车记录了自己的notificationURI型机车供另一个消费者使用,因此分析流可以重新定向. 财产A03.8; a038_evil a038_nfc 攻击询问。 *



- 图5。 转会令牌与其使用的订阅无关 。 财产Z03; 攻击查询 z03b. *

拟议修改。 将经授权的消费者携带在访问令牌中(一个额外的资源范围,指代订阅者或consumerId),拥有NRF仅为它授权的(主体,消费者)配对发行,并设定目标.NWDAF拒绝 aPOST或 时 间PUT谁的身体consumerId与该标志的消费者或资源储存的消费者不同,aDELETE其标志不是用于资源存储的消费者.check_fix{\fn黑体\fs22\bord1\shad0\3aHBE\4aH00\fscx67\fscy66\2cHFFFFFF\3cH808080} 装订的 pv 验证攻击查询 z0310_nfc(并)z03b,a038_nfc)并保持正常运行.

用 ProVerif复核。 该改动已纳入模型的复制件中: 消费者携带进入信使(access acident)consumerId(a) 其主体被授权转让; 编号NRF仅为这对(主体、消费者)发放代币; 目标NWDAF请求consumerId输入 aPUT以等值于象征物的消费者和资源储存的消费者,并且要求DELETE用来为资源存储的消费者携带一个符号。 在改变的模型上ProVerif证明`z0310_nfc`:攻击已经不可能在那里了. 协议的正常运行仍然被找到. 在其它有记录的答案中 ,15 仍然坚守 3 已更改 `:z03b`(A03(a) 被攻击) 现已得到核实;`z03b`(Z03(a) 被攻击) 现已得到核实;`a038_nfc`(A03.8现在已经核实。 这是对模型的首次检查:它显示改变可以消除那里的攻击,而不是它没有引入其他问题. 已更改模式 `:records/fixes/0050-fix-binding.pv`.

这些攻击没有给出数字的发现:A03.8:z0310_nfc,A03.8:z03b,A03:a038_nfc,A03:z0310_nfc,Z03.10:a038_nfc,Z03.10:z03b,Z03:a038_nfc,Z03:z0310_

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	**已接受的转移请求与发送方一致。** 目标 NWDAF 每次接受一次迁移请求（PREPARE 或 TRANSFER），都存在源 NWDAF 的一次真实运行，双方对订阅标识、consumerId、notificationURI 与 transReqType 一致。	无	不成立（2 个攻击）	中	不确定

ID	性质	假定的泄露	结果	价值	文稿是否已写
A04	**在每项移交请求中,多数执行一次。** 目标 NWDAF 对同一迁移请求（同一 transferId / 同一订阅）至多接受一次执行；每次接受对应源 NWDAF 的不同运行。	无	在一个约束内持有(变化中的数值未滚动到4步)	中	不确定
Z01	**只有在得到有效授权的情况下才接受转让。** 每次迁移请求被目标 NWDAF 接受并提交，都必须有授权服务器签发的、覆盖 转让范围 且主体与 consumerId 相符的有效许可。	无	成立	中	是
Z03	**与消费者和转移资源挂钩。** 迁移请求中使用的许可，其主体、受众、资源（订阅/transferId) 与动作（ 转让) 必须与请求体中的 consumerId 和 notificationURI 一致。	无	不成立（1 个攻击）	高	不确定
S04	**不得在转让方面混合使用。** TRANSFER 执行阶段使用的订阅内容与 consumerId/notificationURI 必须来自同一迁移请求的 PREPARE 阶段或同一请求体，不得与其他迁移或订阅的上下文混接。	无	成立	低	不确定
S05	**取消或删除后不执行。** 迁移资源被取消或执行删除之后，使用旧 transferId 或旧迁移上下文不得再提交新的迁移执行或数据收集动作。	无	在一个约束内持有(变化中的数值未滚动到4步)	中	不确定
D01	**被接受的字段是发件人自己的值。** 目标 NWDAF 接受的每个迁移请求字段（transReqType、nwdafEvSub、consumerId、notificationURI）都对应源 NWDAF 的真实发送，未被中间人替换。	无	成立	低	是
A03.8	**目标存储来源订阅和notificationURI.** 目标 NWDAF 接受迁移后，其持有的订阅与 notificationURI 必须与源 NWDAF 请求中的一致。	无	不成立（2 个攻击）	高	不确定
S04.9	**未根据陈旧的转让情况发出通知。** 取消或更新迁移请求之后，在途通知不得再按已失效的迁移上下文提交。	无	在一个约束内持有(变化中的数值未滚动到4步)	低	不确定
Z03.10	**恶意NF不能转让他人的订阅。** 持有自身合法令牌的恶意 NF 不能提交 consumerId 为其他消费者的迁移请求并被接受。	无	不成立（2 个攻击）	高	不确定
X01	**移交请求对网络数据保密。** 只持有网络的攻击者不能获得用于传输请求的进入令牌,也不能获得其携带的订阅标识符和 notificationURI。	无	成立	低	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: 旧订阅与新 NWDAF/notificationURI 关联	对于来源的NWDAF自己转帐,目标记录了确切的订阅内容和发送来源的notificationURI,但协会没有受到其他NF的保护:任何NF带有有效转帐符的,都可以为消费者nfc写一张映射图,并更换其notificationURI(A03.8,Z03.10).	A03.8, Z03.10, Z03
Q2: 迁移请求取消/更新与在途通知的有限状态一致性	在取消转让资源后,目标不会在取消的上下文下就四个未滚动步骤(S04.9,S05)发出待发通知; 从损失的204中恢复,且已在数据源排队的通知没有建模。	S04.9, S05, A04
Q3: 恶意合法 NF 不能把其他消费者订阅迁移到自己	编号:一个合法的NF,并带有自己的有效传动镜信号,可以提交一个传动,命名另一个消费者的consumerId,并让目标接受和执行,因此消费者的notificationURI可以被重定向到攻击者身上(Z03.10,A03,Z03,A03.8)。	Z03.10, A03, Z03, A03.8

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:

- 象征式模型修补了密码原生物; 它不能证明计算强度或量子后强度(C08和算法要求不可问).
- 可得性、时间、进展、僵局和资源消耗都不属于微量财产证明的答案(V01、V02、V03)。
- TLS财务报告和财务报告OAuth2密钥、 令牌过期、 撤销和NRF本身是抽象地模拟的; 编号NRF信得过,而信得过,则视为未过期。
- 转移资源未滚动为四个步骤; 实际删除、持久性、缓存和共享资源表没有模拟任何会议。
- 假定恶意NF人知道consumerId及其受害人的解析器订阅标识; 如果这些是秘密的, 攻击还需要一步来学习它们。
- 通过SCP或SEPP的间接通信,漫游和NEF路径已超出范围; 3. 该型号假设直达NF-to-NF通信.
- 同名订阅赛,每次执行一次的两次转会请求,在国家审查中被确定,但未通过查询确认.
- 部分接受分支(PartialAnalyticsSubTransfer)和部分失败上的无回旋行为没有模型化.
- Tamarin+ Agent(Tamarin+ Agent)以真实的删除语义来模拟一个变化中的资源表,它将解决状态审查候选人和相同的订阅竞争.

主持人记录的是什么:

- A04,S05,S04.9的答案是建立在简化型号的操作上(附录D).

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:接受转移请求者同意其转移请求

目标 NWDAF 每次接受一次迁移请求（PREPARE 或 TRANSFER），都存在源 NWDAF 的一次真实运行，双方对订阅标识、consumerId、notificationURI 与 transReqType 一致。

对于源的NWDAF,目标接受由源的自身发送支持,任何网络攻击者都无法改变一个场; 被接受的字段等于源的值。 对于不同的NF协议,协议失败了:拥有自己有效转帐凭证的NF获得消费者认购的接受,尽管来源从未发送过。

- 结果:失败(2次攻击); 回答问题:是的; 可用备注
- 价值介质:协议部分是原始平原下中央担保的证明; 另有NF人的失败是所有权认定,而文件仅提到所有权认定是一般性警告(ts-29-501 1801),而不是这一程序的失败。
- 在文件中说明:不明确。 资料来源:ts-29-501:1801。
- 休息时间: TLS是双向认证的加密; 标志是不可原谅的 NRF 签名。 ; 唯网解答是一个限于来源转移的查询,因为恶意的NF的证书存在于同一个模型中. ; 没有这NF的TLS密钥和标志,任何攻击者都无法充当NF.
- 开放:目标是否有拒绝consumerId的本地政策,并不服务.
- 下一步:制定部署政策,规定consumerId对电话NWDAF具有约束力,并重新提出第二项主张。

A04:每次转移请求最多一次执行

目标 NWDAF 对同一迁移请求（同一 transferId / 同一订阅）至多接受一次执行；每次接受对应源 NWDAF 的不同运行。

执行时删除了转移资源,aTRANSFER由网络重新传送,或用相同的方式重复transferId,没有被第二次执行; 财产为四个未卷的台阶所持有。 离开资源状态检查的控件会执行两次,所以属性取决于该检查.

- 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
- 价值介质:s0021、s0036和s0047的资源寿命周期意味着财产,但文件没有明确说明重复执行规则。
- 在文件中说明:不明确。 资料来源:s0021、s0036、s0047。
- 休息:目标未滚动为四个消息步骤; 一个真正的资源表没有模拟任何会议的次数。 ; 目标以资源状态(ts-33-501 2875)验证一个消息. ; 每条未滚动链有一个转移请求; 两个请求之间的相同订阅比赛不是模拟的。
- 打开 : 每执行一次, 有两次相同的订阅请求 。
- 下一步:为同一订阅打开两个资源,并询问每个订阅的读数.

Z01: 仅经有效批准才接受转让

每次迁移请求被目标 NWDAF 接受并提交，都必须有授权服务器签发的、覆盖 转让范围 且主体与 consumerId 相符的有效许可。

每一次接受的转让都携带一份完整无缺的NRF-枚标牌,目标为NWDAF作为受众,Nnwdaf-events订阅:转让范围; 网络或另外的NF号申请不予接受。

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:基线要求资源服务器在允许访问前验证符号,其范围和到期,文档说明传输范围.
- 在文件中说明:是的。 这些文件都说:ts-33-501:8014,ts-29-500:4994,s0179,s0180,s0184

- 记号是固定的NRF键下的签名; 撤销和失效不是模拟的。 ; NRF型机车可信,范围为固定常数. ; NRF号机车在认证了NF号机车后,才假定才发行该代币.
- 打开: 已过期或已撤销的令牌 。 ; 观众和主体检查是仿制的,过期检查不是.
- 下一步:添加符号寿命和撤销事件并重新任务.

Z03:与消费者挂钩和转让资源

迁移请求中使用的许可，其主体、受众、资源（订阅/transferId) 与动作（ 转让) 必须与请求体中的 consumerId 和 notificationURI 一致。

信使号与呼叫NF号及目标NWDAF号正确结合,转移范围涵盖行动. 它不受消费者或订阅人的约束:一个信物持有者可以给任何consumerId和notificationURI命名,因此财产的资源部分失效.

- 结果:失败(1次攻击); 回答问题:部分; 可用备注
- 价值高:文件警告说,服务级别的范围不得给消费者不当的写作或删除访问权限,并要求额外的范围来匹配操作,但文件并未说明该程序没有约束消费者或订阅.
- 在文件中说明:不明确。 资料来源:ts-29-501:1801,ts-33-501:8040。
- 补充:来源文本定义不授权使用资源; 该模型给了恶意的NF 自己的有效标志。 ; 托肯过期和撤销不是模拟的。 ; 仅网络资源诉求的答案是将查询限制在来源的传输.
- 打开:操作员的本地策略是否添加了每个资源检查.
- 下一步: 检查的固定装订 。 pv显示每个消费者的代币可以清除失败.

S04: 不得在转移情况下混合

TRANSFER 执行阶段使用的订阅内容与 consumerId/notificationURI 必须来自同一迁移请求的 PREPARE 阶段或同一请求体，不得与其他迁移或订阅的上下文混接。

只有在NF相同的transferId所创造的资源上执行转移,所以执行的上下文属于该转移请求,而不是另一个请求; 2. 没有发现与网络或另外NF的交叉文字混合。

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:资源代表一项转让订阅请求和transferId确定的资源的PUT行为,但文件没有明确说明跨文本规则.
- 在文件中说明:不明确。 资料来源:s0086、s0087、s0088、s0032。
- 休息时间:模特儿。 pv 绑定每个转移到一个线性会话; 资源不是共享的表格。 ; 同一消费者的两个转移请求之间的交叉资源竞争并不是模拟的。
- 打开:同一订阅的第二个传输请求.
- 下一步:解开两个资源,并测试同一订阅是否两次执行.

S05:取消或撤销后不执行

迁移资源被取消或执行删除之后，使用旧 transferId 或旧迁移上下文不得再提交新的迁移执行或数据收集动作。

随着执行时或取消时的资源被移除,与旧transferId重播的TRANSFER被否决,因此对于四个未滚动步骤在移除后不会发生处决. 没有资源状态检查的控制会执行重播,所以属性取决于该检查.

- 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:文档在执行和取消时删除资源,基线需要对照网络状态进行验证,但是没有说明日后重新使用transferId的规则.
- 在文件中说明:不明确。 资料来源:ts-33-501:2875、s0036、s0045、s0047。
- 休息:目标未滚动为四个消息步骤; 真实的删除, 持久性和缓存没有建模 。 ; 目标对照网络状态验证所收到消息.
- 公开:失落的204使源头重新转发并被拒绝.

- 下一步:模拟丢失的响应和来源的恢复.

D01:接受字段是发送者自己的值

目标 NWDAF 接受的每个迁移请求字段（transReqType、nwdafEvSub、consumerId、notificationURI）都对应源 NWDAF 的真实发送，未被中间人替换。

被接受的转让请求的每个字段都等于来源NWDAF发送; 在网络中处于中间的人不能替换transReqType,nwdafEvSub,consumerId或 时 间notificationURI.

- 结果:持有; 回答问题:是的; 可用
- 价值低:基线要求消费者和生产者在NF次服务与TLS次请求保护之间相互认证; 文档定义字段。
- 在文件中说明:是的。 文件中说:ts-33-501:8012,s0010,s0012,s0013,s0014
- 休息时间: TLS是双向认证的加密; 符号是一个不可原谅的签名。 ; 无论是源头还是目标的长期密钥都没有受损.
- 下一步:在所述模式内不需要任何人。

A03.8:目标存储来源订阅和notificationURI

目标 NWDAF 接受迁移后，其持有的订阅与 notificationURI 必须与源 NWDAF 请求中的一致。

对于来源的NWDAF转帐,目标准确记录了来源的订阅和notificationURI. 但任何NF带有有效转移令牌的,都可以使目标记录成为消费者nfc自己的notificationURI,因此消费者的映射可以被接管.

- 结果:失败(2次攻击); 回答问题:是的; 可用备注
- 价值高:文件要求nwdafEvSub必须包含notificationURI和consumerId号标注消费者名称,但文件并未说明目标将notificationURI号标注在该消费者身上.
- 在文件中说明:不明确。 资料来源:s0013、s0014、s0152。
- 目标路线通知consumerId; notificationURI号机的所有权没有检查,因为源文本名称只有consumerId。 ; 订阅识别码和consumerId作为恶意NF可供使用.
- 开放:目标是否有先前的消费者对URI绑定.
- 下一步:在目标处添加一个消费者对notificationURI绑定并重置任务.

S04.9:在陈旧的转让背景下没有通知

取消或更新迁移请求之后，在途通知不得再按已失效的迁移上下文提交。

在取消转让资源后,目标不会发出关于该订阅的待发通知; 没有资源状态检查的控件确实提供了它,所以财产取决于去除.

- 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:取消的传输会移除资源,数据不再需要,但文件没有说明飞行中通知的规则.
- 在文件中说明:不明确。 资料来源:s0045、s0046、s0047。
- 休息:目标未滚动为四个步骤,飞行通知是模拟一个待通知步骤。 ; 在数据源中已经排队的通知没有建模。
- 打开: 已在数据源处飞行的通知 。
- 下一步:在数据源和取消命令中模拟队列。

Z03.10:恶意的NF不能转让他人的订阅

持有自身合法令牌的恶意 NF 不能提交 consumerId 为其他消费者的迁移请求并被接受。

攻击成功:用自己的有效转移镜标志,合法的NF获得目标接受和执行转移,命名为consumerIdnfc,目标记录攻击者为该消费者的notificationURI. 象征性支票对打电话者和范围有约束力,但对消费者或订阅者没有约束力。

- 结果:失败(2次攻击); 回答问题:是的; 可用
- 价值高:文件警告说,服务级别的范围不得给予不当的书写或删除访问权限,附加的范围必须与操作相符,但文件没有说明这一程序没有约束消费者或描述攻击.
- 在文件中说明:不明确。 资料来源:ts-29-501:1801、ts-33-501:8040、s0014、s0020、s0022。
- 休息:恶意NF拥有自己的有效标志,如任何合法的NF一样. ; consumerId和订阅识别码已知或可推断给攻击者. ; 光是网络是办不到的,因为它缺少NF的TLS的密钥和信物.
- 开放:地方目标政策是否会拒绝consumerId美元不服务。
- 下一步:检查每个消费者的代币固定:check_fix显示z0310_nfc在固定装订上得到验证. 页:1

X01: 网络上保密的传输请求数据

仅持有网络的攻击者不能获得用于传输请求的访问令牌,也不能获得其携带的订阅标识符和notificationURI.

仅持有网络的攻击者没有获得访问令牌,订阅标识符或来源的转移请求的notificationURI.

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:OAuth2出入证必须在TLS以上过境时保密,服务请求由TLS在基线中保护.
- 在文件中说明:是的。 文件上说:rfc6749:2859,ts-33-501:8012,s0013,s0152
- 休息时间:TLS系仿制成双向密钥下的加密; 未提出计算或定量主张。 ; 端点没有受损。
- 下一步:在所述模式内不需要任何人。

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_src	检查	a03_any (holds_in_source); z03b (holds_in_source)	证实1,2次攻击
A04	bounded	未滚动到 4 步的数值变化	a04	检查		2 已定界
Z01	proved		z01	检查		证明:1
Z03	proved		z01	检查	z03b (holds_in_source)	证实3,1次攻击
S04	proved		s04	检查		证明:1
S05	bounded	未滚动到 4 步的数值变化	s05	检查		2 已定界
D01	proved		a03_src	检查		证明:1
A03.8	proved		a038_src	检查	a038_evil (holds_in_source); a038_nfc (holds_in_source)	证实1,2次攻击
S04.9	bounded	未滚动到 4 步的数值变化	s049	检查		2 已定界
Z03.10	无				z0310 (holds_in_source); z0310_nfc (holds_in_source)	2次攻击
X01	proved		x01_tok	检查		证明:3

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	每次传送目标NWDAF来源接受NWDAF带有订阅标识符,consumerId,notificationURI财务报告和财务报告transReqType举报人发来的消息; 单凭网络 源头是唯一的NF他们的转学可以被接受。	`network`	proved	a03_src	检查
A03	每一次被接受的转帐都得到NWDAF源的真实运行支持:只有NWDAF源可以让目标接受一个转帐来订阅.	`malicious_nf`	攻击 (holds_in_source)	a03_any(控制 a03_src) (中文(简体)).	
A03	每一次被接受的转让,都命名消费者的订阅(consumerId= nfc) 由源的真实运行支持NWDAF为了那笔订阅费	`malicious_nf`	攻击 (holds_in_source)	z03b(控制 a03_src) (中文(简体)).	
A04	每个转移请求最多一次执行(同transferId):资源执行和移除后网络转发的TRANSFER次没有第二次执行.	`network`	定界(变化中的数值未滚动为 4 步)	a04	检查
A04	每项转移请求最多执行一次(同transferId次):资源状态检查拒绝重复的TRANSFER,同一transferId,无论NF发送它.	`malicious_nf`	定界(变化中的数值未滚动为 4 步)	a04	检查
Z01	每一份被接受和承诺的转移请求都带有NRF号发出的访问令牌,其完整性完好无损,其受众为NWDAF号目标,其范围为nwdaf-events订阅:转移.	`malicious_nf`	proved	z01	检查
Z03	订阅和转移请求中的notificationURI是授权代销对象转让的(请求名称是消费者的订阅和属于该消费者的notificationURI)。	`malicious_nf`	攻击 (holds_in_source)	z03b(控制 a03_src) (中文(简体)).	
Z03	信使的主体是经认证的NF服务消费者,其受众是目标为NWDAF(仅凭网络就可以信使只能是来源).	`network`	proved	z01	检查

目标	主张	攻击者	回答	查询	对照
Z03	信物的主体是认证的NF服务消费者,其受众是NWDAF的目标.	malicious_nf	proved	z01	检查
Z03	请求中的订阅费和notificationURI是授权请求的发送人转移的订阅费; 2. 仅凭网络,消费者订阅的唯一接受转帐是来源NWDAF自己的.	network	proved	a03_src	检查
S04	仅在为同一目的创建的传输资源上执行传输transferId以相同方式NF; 执行的上下文属于该转移请求,而不是属于另一个请求。	malicious_nf	proved	s04	检查
S05	转让资源被取消后,与旧transferId重播的TRANSFER没有执行.	network	定界(变化中的数值未滚动为 4 步)	s05	检查
S05	在转让资源被取消后,与旧transferId重播的TRANSFER没有执行,无论重播来自网络还是来自持有transferId的NF.	malicious_nf	定界(变化中的数值未滚动为 4 步)	s05	检查
D01	接受的转移请求的每个领域(transReqType、nwdafEvSub、consumerId、notificationURI)均相当于来源NWDAF发出的请求; 在网络中处于中间的人不能取代一个值。	network	proved	a03_src	检查
A03.8	对于来源的NWDAF转帐,订阅识别码和notificationURI,目标记录正是来源在nwdafEvSub中发送的记录.	network	proved	a038_src	检查
A03.8	只有来源NWDAF才能使目标为消费者记录notificationURI; 目标为消费者绘制的地图总是符合来源的要求。	malicious_nf	攻击 (holds_in_source)	a038_evil(控制a038_src) (中文(简体)).	
A03.8	只有来源NWDAF才能使目标记录消费者nfc的notificationURI; 目标为消费者绘制的地图总是符合来源的要求。	malicious_nf	攻击 (holds_in_source)	a038_nfc	
S04.9	在转让资源被取消后,在取消的转让上下文下不会发出飞行中通知。	network	定界(变化中的数值未滚动为 4 步)	s049	检查
S04.9	在取消一项转移资源后,在取消的转移语境下,无论是从网络还是从NF号机上取消,都不会发出飞行中通知.	malicious_nf	定界(变化中的数值未滚动为 4 步)	s049	检查
Z03.10	持有自己有效证书和转移范围的NF例不能使目标NWDAF接受转移,以命名另一个消费者的订阅/consumerId.	malicious_nf	攻击 (holds_in_source)	z0310	
Z03.10	持有自己有效证书和转移范围的NF例不能使目标NWDAF接受以consumerId=nfc命名消费者订阅的转移.	malicious_nf	攻击 (holds_in_source)	z0310_nfc	
X01	用于源的传输请求的访问符不是由只持有网络的攻击者获得的.	network	proved	x01_tok	检查
X01	来源传输请求中携带的订阅标识符不是只持有网络的攻击者获得的.	network	proved	x01_sub	检查
X01	在来源的转移请求中携带的notificationURI不是只持有网络的攻击者获得的.	network	proved	x01_uri	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-20261114T234529, 2026-11-14. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:64,校对:7 s,壁25 min,耗资0.221 USD.

背景:主机从谈话中移除了1时间(s),总共删除了544666个字符(更早的推理,以及最新变化之前显示模型的内容)的僵化部分. 轨迹文件保存了一切

ProVerif:127 证明运行,127 决定,0 未答,5 s,38 答录.

分析了什么

协议	NWDAF 分析订阅转账控制
版本	19.8.0
分析范围	两个 NWDAF与一个既有 NF消费者;固定单个非 UE聚合 分析订阅，创建/更新/取消一次 转移请求及相关确认；保留 原始订阅与目标 notificationURI映射，排除用户移动与 上下文获取全流程。
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209个编号段落(162115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	4.2.2.5	Nnwdaf_EventsSubscription_Transfer次服务业务
主体	4.2.2.5.1	A. 概况
主体	4.2.2.5.2	创建分析订阅转让请求
主体	4.2.2.5.3	更新分析订阅传输请求
主体	4.2.2.5.4	取消关于分析订阅传输的请求
主体	5.1.1	导言
主体	5.1.2	使用费HTTP美元
主体	5.1.2.1	A. 概况
主体	5.1.2.2	HTTP标准标题
主体	5.1.2.2.1	A. 概况
主体	5.1.2.2.2	内容类型
主体	5.1.2.3	HTTP 个自定义标题
主体	5.1.3.1	资源结构
主体	5.1.3.4	资源:NWDAF 事件订阅转让
主体	5.1.3.4.1	说明
主体	5.1.3.4.2	资源定义
主体	5.1.3.4.3	资源标准方法

文稿	章节	标题
主体	5.1.3.4.3.1	POST
主体	5.1.3.4.4	资源自定义操作
主体	5.1.3.5	资源:个人NWDAF事件订阅转让
主体	5.1.3.5.1	说明
主体	5.1.3.5.2	资源定义
主体	5.1.3.5.3	资源标准方法
主体	5.1.3.5.3.1	DELETE
主体	5.1.3.5.3.2	PUT
主体	5.1.3.5.4	资源自定义操作
主体	5.1.6.2.40	AnalyticsSubscriptionsTransfer型机车
主体	5.1.6.2.41	SubscriptionTransferInfo型机车
主体	5.1.6.2.43	AnalyticsContextIdentifier型机车
主体	5.1.6.2.49	ConsumerNfInformation型机车
主体	5.1.6.3.17	编号: TransferRequestType
主体	5.1.7	处理错误
主体	5.1.7.1	A. 概况
主体	5.1.7.2	协议错误
主体	5.1.7.3	应用程序错误
主体	5.1.8	特性谈判
主体	5.1.9	警卫

协议的目的是在文档中将其定位为源步骤:两个 NWDAF与一个既有 NF消费者;固定单个非 UE聚合 分析订阅，创建/更新/取消一次 转移请求及相关确认；保留 原始订阅与目标 notificationURI映射，排除用户移动与上下文获取全流程。

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	接受转移请求者同意其发送者的意见	目标NWDAF和转移的NF服务消费者(来源NWDAF):目标接受转移请求(PREPARE或TRANSFER),由持相同订阅识别码的该消费者真实发送,consumerId,notificationURI和transReqType支持.	信息流有来源NWDAF发送AnalyticsSubscriptionsTransfer机体,目标NWDAF对此采取行动(s0007,s0010,s0020,s0022); 在s0012..s0014和s0152中界定了有关领域。 这些文件没有说明明确的协议财产; 请求/答复流量超过经认证的TLS(ts-33-501 8012, ts-29-500 4994)就暗示了这一点。	s0003, s0007, s0010, s0014, s0020, s0022, s0152
A04	每项转移请求最多一次执行	目标NWDAF: 一个个人NWDAF事件订阅传输资源(1)transferId,一个订阅))最多执行一次,每次执行匹配一个不同的运行NF服务消费者。	PREPARE美元创造了一次资源(s0021); a TRANSFER(POST或PUT)执行并删除资源(s0024、s0036、s0037); a DELETE将其删除(s0045,s0047). 文件没有阐明重复执行规则; 资源生命周期意味着它。	s0021, s0024, s0036, s0037, s0045, s0047

ID	简称	对象	文稿怎么说	出处
Z01	只有经有效授权才接受转让	目标NWDAF(资源服务器):每个接受和承诺的传输请求都携带NRF(授权服务器)发布的访问令牌,完整性完整无缺,覆盖nwdaf-events订阅:传输范围.	这些文件授权以NRF为授权服务器的Nnwdaf_EventsSubscription API至OAuth2客户证书,并规定了转移范围(s0179、s0180、s0182、s0184); 基线由资源服务器核查该信物、其范围和有效期(ts-33-501 8014、8038、8042); ts-29-500 4994).	ts-33-501:8014, ts-29-500:4994, s0179, s0180, s0182, s0184
Z03	与消费者和转移资源挂钩	目标为NWDAF和consumerId命名的分析消费者:该信物的主体是经过认证的NF服务消费者,其受众是目标为NWDAF,请求中的订阅和notificationURI是授权转让的对象.	基准封面上标明的代号检查对TLS00人的身份、观众对生产者和范围/额外范围对要求的操作(ts-33-501 8028、8032、8038、8040); 文件还警告说,服务级别的范围不得允许不适当的书写或删除对不当消费者的访问(ts-29-501 1801、1795)。 consumerId识别订阅的消费者(s0014,s0152).	ts-33-501:8040, ts-29-501:1801, s0014, s0117, s0152, s0184
S04	不得在转让背景中混合	目标NWDAF和来源NWDAF:执行转帐时使用的订阅内容consumerId和notificationURI属于同一个转帐请求(同transferId),而不是另一个转帐或订阅.	这笔资源是调用订阅费的请求(s0086、s0087、s0088、s0111); a PUT更新了transferId确定的资源,并执行(s0030、s0032、s0036)。 文件没有明确说明交叉文本规则。	s0086, s0087, s0088, s0032, s0036, s0046, s0047
S05	取消或删除后没有执行	目标NWDAF:在转移资源被移除(取消DELETE或被执行的TRANSFER)后,一个旧的transferId或旧的转移语境不再被接受执行或数据收集.	目标删除执行时和取消时的资源(s0036,s0037,s0045,s0047),并在不再需要时删除数据/未订阅(s0046). 基准要求每个NF对照协议和网络状态验证收到的电文(ts-33-501 2875).	ts-33-501:2875, s0036, s0037, s0045, s0046, s0047, s0048
D01	接受字段是发件人自己的值	具体目标NWDAF:经接受的转移请求的每个领域(transReqType、nwdafEvSub、consumerId、notificationURI)均相当于经认证的发送者发出的转移请求; 中间没有人能取代价值	在s0010..s0014和s0020中界定了身体领域; 基线以TLS和象征性授权(ts-33-501 8010、8012、2871)保护请求; ts-29-500 4990, 4994).	ts-33-501:8012, s0010, s0012, s0013, s0014, s0020, s0022
A03.8	目标储存了来源的订阅和notificationURI	目标NWDAF和分析消费者:在接受转让后,目标持有订阅,并将通知notificationURI,这是nwdafEvSub年发出的来源NWDAF,其中必须包含最初的notificationURI。	转移机载nwdafEvSub,内装notificationURI型(s0013,s0152,NOTE),目标执行转移(s0022). 这些文件没有说明对超过consumerId(s0014)的消费者约束notificationURI的规则。	s0013, s0152, s0022, s0014
S04.9	没有在陈旧的转让语境下发出通知	目标NWDAF和分析消费者:在取消或更新转让请求后,不在取消或替换的转让上下文下发送飞行中通知。	取消的转账将删除不再需要的资源和数据,不订阅数据来源(s0045、s0046、s0047); 文件没有说明飞行中通知的规则。	s0032, s0036, s0045, s0047

ID	简称	对象	文稿怎么说	出处
Z03.10	恶意的NF不能转移别人的订阅	consumerId命名的分析消费者和NWDAF的目标:持有自己有效证书和转移范围的NF个实例不能提交转移请求,命名另一个消费者的订阅consumerId并让目标接受.	consumerId是即将转让的订阅的消费者的NF实例标识(s0014); 转移范围是授予转移业务的服务级范围(s0184),文件警告说,服务级范围不得给不适当的消费者写作或删除访问权限(ts-29-501 1795,1801),资源服务器必须对照操作检查额外范围(ts-33-501 8040)。	ts-29-501:1801, ts-33-501:8040, s0014, s0184
X01	在网络上保密的传输请求数据	来源:NWDAF,目标:NWDAF 分析消费者:转移请求机身(订阅,consumerId,notificationURI)和随机出行的接入符,只有网络的攻击者无法读取.	TLS00以上(rfc6749 10.3、P011-P015)的出入证过境时必须保密; 转移机携带分析机订阅及其notificationURI(s0013,s0152),基线以TLS(ts-33-501,8012,ts-29-500,4994)保护服务请求.	rfc6749:2859, ts-33-501:8012, s0013, s0152

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 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 29 段，没选 369 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	OAuth2项安全考虑的导言; 它指出,这些措施取决于客户类型和赠款类型,对这项协议没有要求。
P003 至 P006	rfc6749:2790-2823	Z01, Z03, `malicious_nf`	
P007 至 P010	rfc6749:2827-2850	Z03, Z03.10, `malicious_nf`	
P011 至 P015	rfc6749:2859-2881	Z01, Z03, X01, `network`, `malicious_nf`	
P016 至 P033	rfc6749:2885-3003	不在范围内	更新令牌、授权代码、重定向URI操纵和资源所有人密码证书属于NWDAF API不使用的赠款类型; 它使用客户证书赠款(s0179美元)。
P034 至 P036	rfc6749:3013-3028	D01, Z01, X01, `network`	
P037 至 P039	rfc6749:3032-3041	证明器问不了	猜测客户资格,是关于证书和原始的实力,而象征模型并不衡量这些实力.
P040 至 P054	rfc6749:3045-3167	不在范围内	涉及最终用户浏览器的Phishing、跨站点请求伪造、点击劫持、代码注入和打开重定向器; 此程序没有终端用户,也没有浏览器。
P055 至 P062	rfc6749:3170-3210	不在范围内	滥用访问标志冒充资源所有者适用于隐含的赠款,NWDAF API号没有使用.
P063	ts-33-501:2491-2491	证明器问不了	降低安全性能的竞标涉及算法谈判; 象征式模型修补原始人,而不测量其力量。
P064 至 P213	ts-33-501:2495-2853	不在范围内	这些要求是:UE订阅认证、信号保密/完整性、用户隐私和RAN/UDM/AUSF/UDR行为(声明)5.1-5.8); 此任务模式仅包含NWDAF-改为:NWDAF服务操作,而不是5G访问网络。
P214	ts-33-501:2859-2859	不在范围内	信托区和NDS/IP 保护跨越信托边界的信息是部署财产; 该型号假设直接NF-至NF通信由TLS保护.

段落	出处	定为	不选的原因
P215 至 P220	ts-33-501:2865-2875	Z01, Z03, A03, A04, D01, S05, `malicious_nf`	
P221 至 P227	ts-33-501:2879-2891	Z01, `malicious_nf`	
P228 至 P314	ts-33-501:2895-3081	不在范围内	对NEF、SCP、SEPP、漫游中介、属性保护和IPUPS的要求涉及这一任务未涉及的实体和路径; 该模型假设没有SCP/SEPP直接通信.
P315 至 P318	ts-33-501:3085-3091	没有陈述目标	3gpp-Sbi-Originating-Network-Id头条及其配置的处理状态没有为转移程序而必须持有或可以攻击的财产.
P319 至 P337	ts-33-501:3097-3141	没有陈述目标	信号监测和安全可见/配置要求是业务能力,而不是传输信息的财产。
P338 至 P369	ts-33-501:3149-3215	证明器问不了	加密和完整性算法识别符和算法选择是原始人的力量,象征模型不测量.
P370 至 P398	ts-33-501:3219-11901	不在范围内	5G-RG,NSSAAF,N3接口,EAP-TLS,IAB,MBSF/MBSTF和NEF的所需经费涉及其他子系统,而不是NWDAF分析订阅转账.

性质目录，逐条去向

性质是从一份安全和隐私性质目录起草的。起草时有 35 条没选，分析者把它们逐条过了一遍：作为性质在这里检查，或者写明原因不检查。检查了 14 条，没检查 21 条。“文稿没有提到”不能作为不检查的原因。

条目	目录里的性质	作为哪条性质检查	不检查的原因
K01	密钥／凭据保密性	X01	
K02	载荷与端到端保密性	X01	
K03	强保密／秘密值不可区分性	不适用	转移控制显示,consumerId和notificationURI是目标必须使用的识别标志; 不可声称或需要替代秘密值之间的不可区分性,象征性模型只会重复加密。
K04	密钥用途、方向与会话分离	不适用	转让程序本身没有密钥; TLS和OAuth2令牌键是每帕基线材料,范围边界将它们置于本分析之外.
A01	对端曾参与性（寿命)	A03	
A02	弱一致性认证	A03	
A05	隐式密钥认证	不适用	该程序没有设定新的会话密钥,因此隐含的密钥认证不适用.
A06	显式密钥确认	不适用	该程序没有进行关键确认; 201/204的答复是HTTP确认,而不是持有密钥的证据。
A07	身份—凭据—密钥绑定	Z03	
A08	协商参数与安全上下文绑定	S04	
R01	认证／挑战新鲜性	不适用	转让程序没有异议、没有刷卡或时间戳; 新鲜度由transferId资源携带,代号到期.
R02	消息级抗重放	A04	
R03	业务操作至多一次	A04	
R04	消息接受顺序／窗口安全	S05	
R05	抗降级／安全策略保持	不适用	移交程序没有可降低的版本、套件或安全级谈判。
C01	前向保密性（FS）	不适用	程序没有设定会话密钥,因此前向保密不适用.

条目	目录里的性质	作为哪条性质检查	不检查的原因
C02	抗密钥泄露冒充（KCI）	不适用	转让程序中当事人之间没有关键设定,因此关键妥协假冒不适用.
C03	已知密钥安全／泄露隔离	不适用	该程序没有关键等级,其密钥可以隔离.
C04	临时秘密／部分状态泄露韧性	不适用	程序没有规定任何秘密; 唯一的储存状态是S04/S05覆盖的转移资源。
C05	泄露后安全恢复（PCS）	不适用	该程序没有鼠标或重键,因此妥协后的安全性不适用.
C06	注册凭据泄露后的增强认证	不适用	涉及第PAKE号或登记记录。
C07	抗离线字典攻击	不适用	不使用密码或人类选择的秘密; NF证书是密码学密钥,离线词典攻击不适用.
C08	指定原语失效下的目标保持	证明器问不了	当一个被命名的原始失败时,恢复力涉及密码算法的强度,符号模型固定了这个算法而不测量.
Z02	委托权限不扩张	S04	
Z04	撤销与过期生效	Z01, S05	
Z05	跨租户／跨服务安全隔离	Z03.10	
S01	加密 0nonce 唯一性 (中文(简体)).	不适用	转让程序没有使用本身的非敏感原始材料; TLS记录保护为基线.
S02	重传／密钥重安装安全	A04	
S03	抗回滚与状态单调性	S05	
P01	身份匿名性	不适用	NF00个身份在这项程序中得到认证和可见; 不得声称匿名。
P02	会话不可关联性	不适用	移交程序在休会期间没有提出不相关联的主张。
P03	用户／凭据存在性隐藏	不适用	转让资源用其创造者已经持有的不透明transferId处理; 没有任何用户或证书存在查询可以列出答复。
V01	条件性进展／错误恢复	证明器问不了	有条件的进步和恢复是活性问题; ProVerif回答追踪属性,而不是运行是否总是完成.
V02	无非预期死锁	证明器问不了	死锁自由是一个活性问题,即追踪财产证明器不能被问到.
V03	受限资源滥用／抗放大	证明器问不了	资源滥用和扩展是成本问题,超出了计算事件的范围,而这一证明器对此并不加以衡量。

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 20 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 14 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	源 NWDAF	参与方	攻击者得不到更多	来源 NWDAF 是 合法 的 发件人 , 并且 已经 持有 订阅 ; 因为属性 询问了它的折中修改无任何(目标仍然存储源发送的且请求仍然被授权),它执行的任何重定向都已经通过恶意的NF实现.
S02	目标 NWDAF	参与方	按定义全部失守	所询问的关于验收、证物检查、资源状况和储存的绘图的每一个财产都是目标NWDAF的财产; 控制它的攻击者可以接受和记录任何东西, 并且文件不问其中任何一个 在一个失密的制作人。
S03	分析消费者	参与方	攻击者得不到更多	分析消费者是资源拥有者:受损的消费者转移了自己的订阅,房产并不禁止这样做。
S04	NRF	参与方	按定义全部失守	NRF是授权服务器; 控制它的攻击者可以发出任何令牌,所以每个授权属性都按定义丢失,而文件在没有可信赖的授权服务器的情况下询问其中任何一个.
S05	恶意合法 NF	参与方	`malicious_nf`	

ID	参与方或值	类别	攻击者条件	不设的原因
S06	分析 订阅	值	攻击者得不到更多	分析订阅是目标必须持有和使用的对象; 读取它不会打破任何要求的属性(增加的保密目标是针对网络攻击者,恶意的NF会带自己的订阅内容).
S07	consumerId	值	攻击者得不到更多	consumerId是一个公共的NF例标识符,用于路由.
S08	notificationURI	值	攻击者得不到更多	notificationURI是目标必须使用的元数据; 了解其本身不违反协议或授权属性,网络保密目标涵盖其过境。
S09	transReqType	值	攻击者得不到更多	transReqType是一个公开的点数值(E) :PREPARE/TRANSFER).
S10	个人 NWDAF 事件订阅转让 资源	值	malicious_nf	
S11	transferId	值	malicious_nf	
S12	OAuth2 访问令牌	值	malicious_nf	
S13	范围 nnwdaf- events 订阅: 转让	值	攻击者得不到更多	范围名称公开,并在规格(s0184)中注明.
S14	访问令牌	值	malicious_nf	
S15	迁移资源	值	malicious_nf	
S16	订阅内容	值	攻击者得不到更多	订阅内容是目标必须持有的,以便为它服务; 攻击者在自己的要求中带来了自己的内容.
S17	数据源订阅	值	攻击者得不到更多	数据源订阅属于目标数据收集范围,不在模式传输流量之外; 读他们破解 任何财产要求。
S18	迁移请求体字段	值	攻击者得不到更多	传输请求体字段是目标必须处理的信息内容; 攻击者可以把自己的值放进自己的请求中,这就是已经命名的恶意的NF曝光.
S19	订阅	值	攻击者得不到更多	订阅是目标必须持有的对象; 这和S06相同
S20	在途通知	值	攻击者得不到更多	向消费者发出的飞行通知受到TLS的保护; 所询问的这些财产是属于哪个转让背景(S04.9),而不是其秘密。

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		
malicious_nf	合法NF例(与来源NWDAF、目标NWDAF和分析消费者不同),拥有自己的TLS证书和自己的有效OAuth2访问证,用于nwdaf-events订阅:以目标NWDAF为受众的转让范围; 它可以打开TLS到目标,并发送服务请求.	任务范围界限要求用自己的证书来区别恶意合法NF; 转移范围允许进入转移业务(s0184)和基数发放NRF(ts-33-501 8008 8010)的标语。	

ID	network	malicious_nf
A03	成立	不成立
A04	成立	成立
Z01	成立	成立
Z03	成立	不成立
S04	成立	成立
S05	成立	成立
D01	成立	

ID	network	malicious_nf
A03.8	成立	不成立
S04.9	成立	成立
Z03.10		不成立
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。
- S05:在ProVerif中回答,分析师的名字是changing_state。
- S04.9: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
NWDAF事件订阅转让资源,由transferId确定(及其储存的订阅,consumerId和notificationURI)	目标 NWDAF	于POST PREPARE (s0021) 创建,于PUT PREPARE (s0032) 取代,于PUT TRANSFER 处死 (s0036,s0037) 和DELETE 取消 (s0045,s0047) 撤销.	每页PUT财务报告和财务报告 DELETE发往/转让/{transferId),目标必须找到它被要求更新或删除的资源(s0030,s0044);ts-33-5012875需要对照网络状态验证收到的消息	s0021, s0030, s0032, s0036, s0037, s0038, s0044, s0045, s0047, s0049
从分析员订阅费(nwdafEvSub)到notificationURI的地图,以发出通知	目标 NWDAF	资源创建或更新时由转移请求机构编写(s0013、s0152、NOTE); 取消后不再需要,删除数据和不订阅(s0046)	当目标在转移的notificationURI(s0152 NOTE)向消费者发出通知时	s0013, s0014, s0046, s0152
NWDAF(准备、执行或取消)与它收到的transferId号申请一起保存在请求的生命周期中的位置	来源:NWDAF	当它收到201(单位:千美元)PREPARE(s0021,则204(单位:千美元)TRANSFER执行(s0036),或204用于取消(s0048)	在它发出关于同一移交请求的下一次请求之前(s0030、s0044)	s0021, s0030, s0036, s0044, s0048

模式	结果	目标	显示于 ProVerif	步骤
重播(E)	没有找到			资源执行或取消后重新播放的TRANSFER被资源检查拒绝:定界. pv验证s05(除去后不执行死刑)及其控制s05_ctl伪造,a04最多显示每transferId处处决一次. 重播的POST PREPARE被接受,不过它只是用新的transferId创建了新的转移请求,这是POST的普通语义,没有突破目标.
repeat_one_time_action	没有找到			定着界. pv a04 核实最多一次执行一次转移请求; 控制a04_ctl, 支票被忽略, 显示两次处决, 所以财产依赖于资源状态检查。

模式	结果	目标	显示于 ProVerif	步骤
脱同步	候选人		否:没有以ProVerif进行审判	来文方发送了PUT/trans/{transferId}和transReqType TRANSFER(s0035). / 目标执行传输并移除资源(s0036),然后发送204 No Content. / 网络放弃204号机车. / 消息来源转发了同样的PUT; 目标找不到资源并拒绝(s0038,ts-33-501,2875). / 来源现在认为,当目标执行时,转移没有执行,并移除了资源; 来文方无法从取消transferId(s0045、s0047、s0048)中看出处决。
update_before_check	没有找到			目标在改变资源前验证访问符和资源:ts-33-5018014,8038,8046在服务执行前验证该符,s0031-s0036对transferId确定的资源采取行动. 定着界. pv 模拟创建前和每次更改前的符号检查 。
no_rollback_on_failure	候选人		否:没有以ProVerif进行审判	仅部分接受TRANSFER项请求:PartialAnalyticsSubTransfer特征得到支持,并非所有分析事件都得到接受(s0024,s0034,s0037)。 / 目标仍在发送201/200与failTransEventReports(s0024,s0037)后删除个人NWDAF事件订阅传输资源. / 资源已消失,因此消费者无法在同一转移请求下重试或完成失败的事件; 源文本定义了不滚回已准备的资源。
race_between_sessions	候选人	A04	否:没有以ProVerif进行审判	创建了两个相同的分析订阅请求,每个请求都有自己的transferId(s0021,s0022). / 两者都执行,目标在自己执行后(s0036)都会移除每个资源. / 目标目前为同一订阅进行两个数据收集和两个通知流; s0020-s0024或s0031-s0037没有拒绝第二次要求,因为支票是每transferId次,而不是每次订阅一次。
distinguishable_failure	没有找到			目标确实返回了不同的代码(201/204,307/308重定向,以及5.1.7的错误代码),但一个transferId是一个不透明的手柄,只在创作者的TLS会话(s0105,s0117)内返回,所以故障代码不能显示消费者的身份或目标询问的值. 没有目标取决于它。
wrap_or_window	没有找到			变化中的值是一个不透明的transferId字符串(s0117)和请求的生命周期; 没有数字计数器或验收窗口,所以没有东西可以包裹或掉到窗口外.

分析师给目标取了什么名字?

步骤	目标	特性	原因：
33	A04, S05, S04.9	changing_state	这三个目标依赖于个人NWDAF事件订阅转移资源,这一价值会因各个步骤而变化:它由PREPARE创建,经TRANSFER次执行或DELETE次取消而去除,飞行中通知可能在之后仍然可以发出。 ProVerif无法跟踪任何会议次数的资源表,所以模式. pv 绑定每次传输到一个线性会话, 并且这些目标没有被绑定 。 页:1
33	A03, Z01, Z03, Z03.10, D01, A03.8, S04, X01	plain_primitives, many_sessions	TLS是一个双向认证的加密模型,只有它的平庸行为,访问令牌是不可原谅的NRF签名,任何会话都会被问及答案. 除了共享密钥加密之外,没有代数定律被涉及.

分析员的结语

密码11目标得到回答。 仅针对网络,转移控制就应发挥应有的作用:实地完整性和与来源的协议得到证明(D01,A03A. 第一批主张OAuth2证明代用支票(Z01),符号绑定在呼叫者和目标上(.Z03第1项主张),执行的上下文属于其本身的转移资源(第1项主张)S04),符号/订阅/notificationURI保密(X01),且未滚动的目标拒绝执行或取消后重发或重播的传输(A04,S05,S04.9,每个框4步骤与伪造的控制)。

调查结果:一个合法的NF加有自己有效转镜的代号,获得目标NWDAF接受和执行一个转机,命名另一个消费者的订阅,目标记录了攻击者对该消费者的notificationURI(Z03.10,Z03第二次主张,A03第二次主张,A03.8,全部holds_in_source在malicious_nf攻击者之下). 目标检查信物的主体,受众和范围,但与consumerId或订阅者无关. 这些文件只是一般地警告说,一个服务级别的范围不得给予不当的书写权限(ts-29-501 1801,ts-33-501 8040),所以新颖性并不明确,而不是记录下来. check_fix 固定装订。 pv显示拟议固定(令牌中的每个消费者范围加上目标时的consumerId比较)去除攻击并保持正常运行.

未经证实的状态审查结论:丢失的204解除了源与目标同步,部分接受仍然移除资源,两个相同订阅的传输请求各执行一次. 一切依托于列出的简化:固定的原始,没有符号过期或撤销,一个值得信赖的NRF,以及一个未滚动到四个步骤的目标——Tamarin+ Agent(英语:Tamarin+ Agent)会解决状态问题.