ML号示范条文与SBA号隔离审查的安全分析

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; 《服务定义原则和准则》; 3阶段(辅助）; 5G系统的安全结构和程序(辅助）美元)
检查的性质	9 条：3 条成立，6 条不成立（6 个攻击）
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

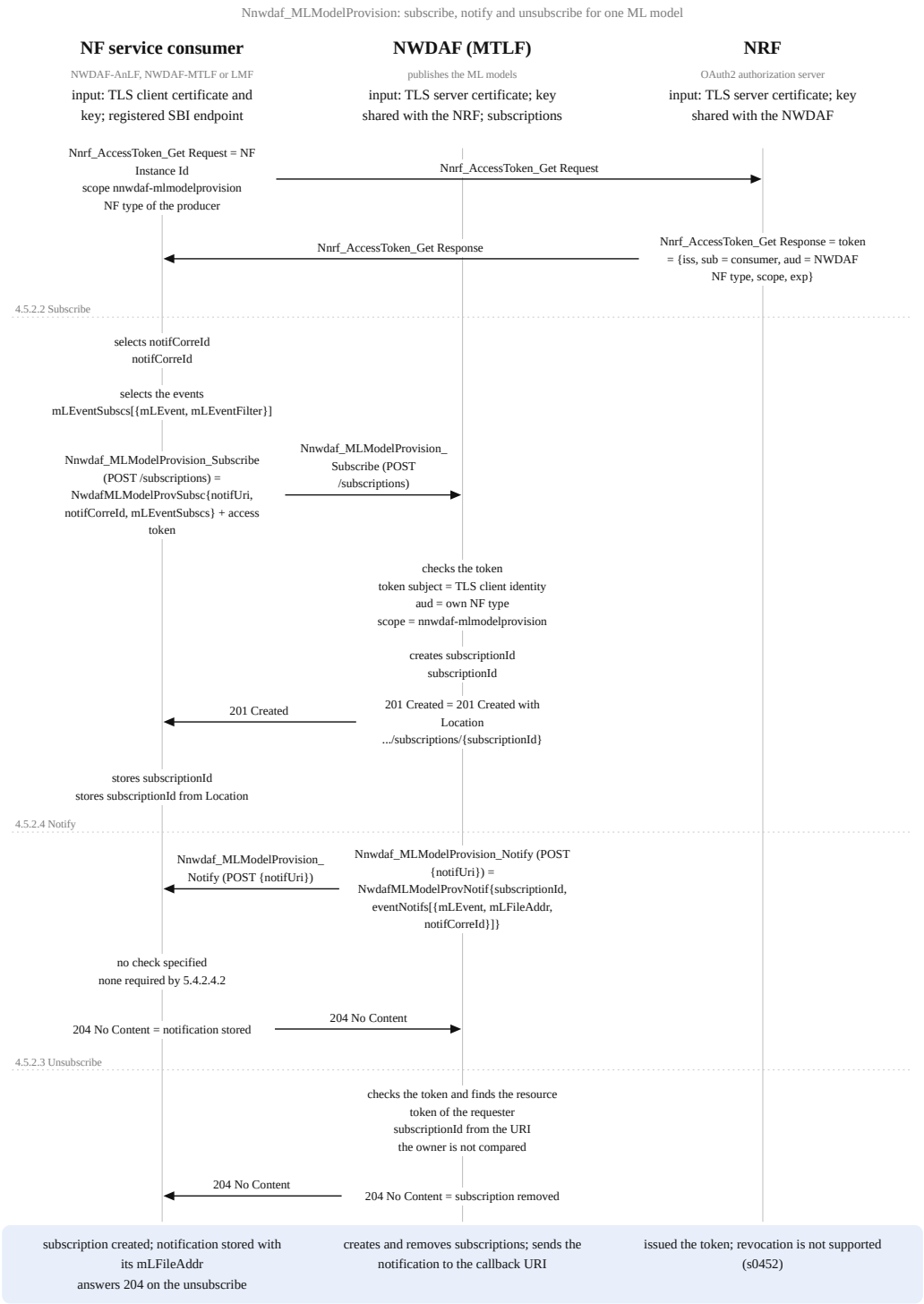
Nnwdaf_MLModelProvision服务让一个NF的服务消费者从NWDAF中获得了ML型号,该型号包含模型的训练逻辑函数而无需携带模型本身:消费者订阅了ML型号事件,并收到一份通知,命名模型和可以获取模型文件的地址. 消费者持有其TLS客户证书,从NRF号机处获得OAuth2号进入证; 2. NWDAF号机持有与NRF号机共用的令牌密钥,并保持订阅; 2. NRF是授权服务器.

消费者以POST的订阅资源订阅,给出了它的回调URI,一个通知关联识别符和它想要的事件. NWDAF号机检查了符号,创建了带有它所分配的标识符的订阅,在位置头返回该标识符,然后张贴一份通知给带有标识符和模型文件地址的回调URI. 消费者存储通知并回答204,当消费者不再想要事件时,消费者会用其标识删除订阅.

双方:

- **NF 服务消费者**:NWDAF-AnLF,NWDAF-MTLF或LMF. 持有:TLS客户证书和密钥; 登记了SBI个终点。
- **NWDAF(MTLF)**:出版ML型号. 持有:TLS服务器证书; 与NRF共用的密钥; 订阅.
- **NRF**:OAuth2 授权服务器. 持有:TLS服务器证书; 与NWDAF共享密钥。

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。

在经分析的分流中,运输和OAuth2零件持有:没有一方能够再伪造TLS端点,每个订阅和不订阅NWDAF的处决都有一个NRF的代币作为后盾,这是它所看到的连接的例子。 有两个发现。 注册的NF持有自己的证书和令牌,可以向另一个消费者的回调URI发布通知,消费者用该NF的模型文件地址和关联识别符存储,因为通知业务在OAuth2之外,消费者只需存储其接受的东西. 拥有有效服务镜标志的消费者知道另一个消费者的subscriptionId可以删除该订阅,因为API定义了单一服务范围,未订阅者从不将请求者与所有者进行比较. 两者都被检查为模型上的修改:将通知绑定给制作人和订阅者,并将所有者与未订阅者进行比较,去除攻击而不丢失正常运行或任何其他记录的答案. 所有9个目标都有他们所说的攻击者的答案,除了关于通知内容的每个证据之外,每个证据都有一个控制失效; 其余的答案依赖于限制下所列的简化,主要是理想化的TLS频道和单调订阅商店.

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.

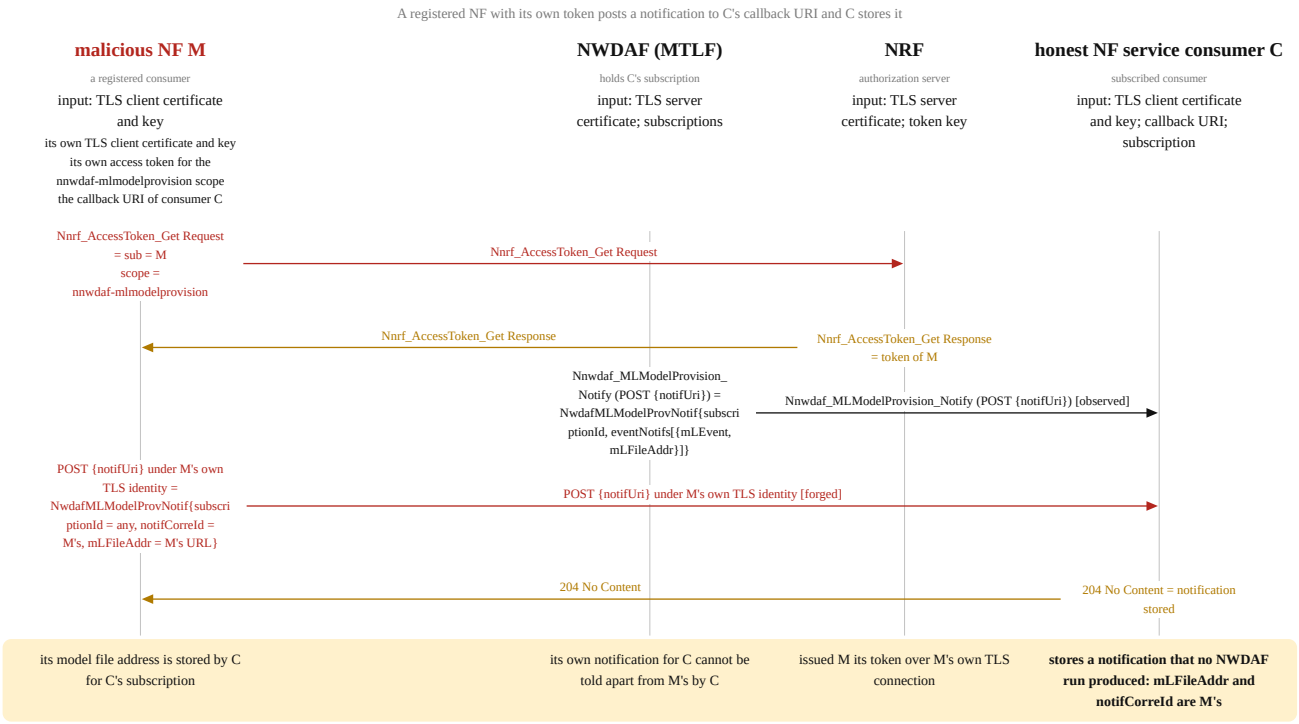
2.1 注册的NF可以在另一个消费者的回调中植入一个模型通知 URI

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-33-501:7892)
价值	中
涉及的性质	A03, A08, A03.7, A08.9 （见第 3 节）
原文	s0108, s0123, s0410
依据	ProVerif 攻击询问 `a03_nf`,`a08_nf`; 图2、3、4和5

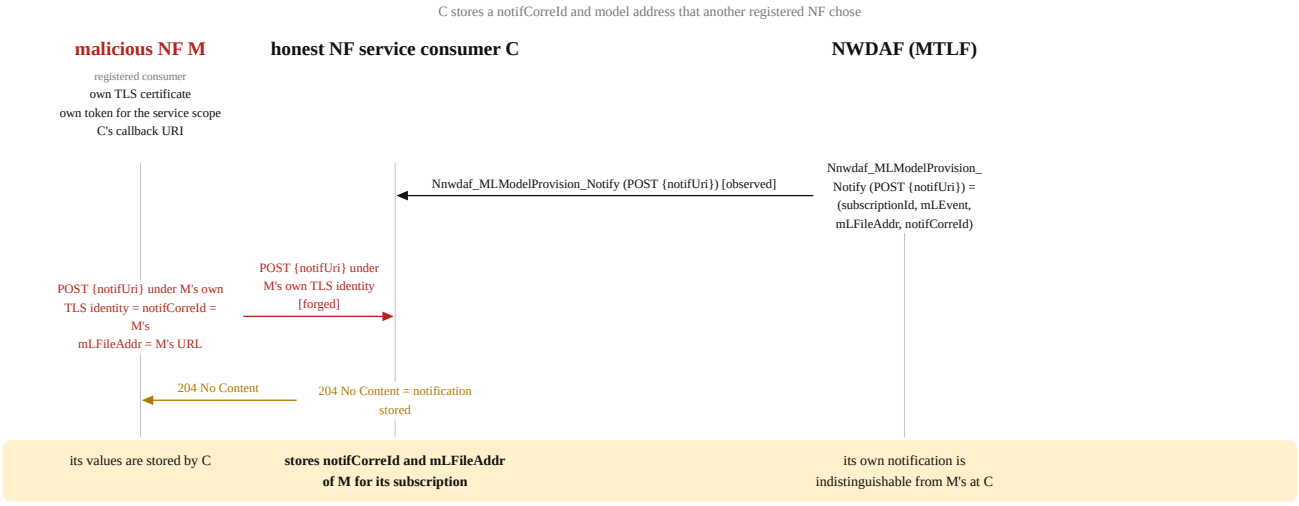
发生了什么。 通知业务没有授权,消费者只需储存其接受的东西,因此运输是其全部防御,运输证明NF发送了信息,而不是NWDAF. 一个恶意的NF通过自己的TLS连接将一个NnwdafMLModelProvNotif形状的机体贴在消费者的召回URI上,消费者用发送者的notifCorreId和模型文件地址存储. NWDAF自行发出的同一订阅通知未受影响,消费者无法将两者区分开来.

攻击者需要什么。 注册的NF服务消费者持有自己的TLS客户证书,自己的NRF-为服务范围签发了访问证,目标消费者注册的回调URI。 回调URI是仿照登记的SBI终点; 攻击者需要它先泄露出来

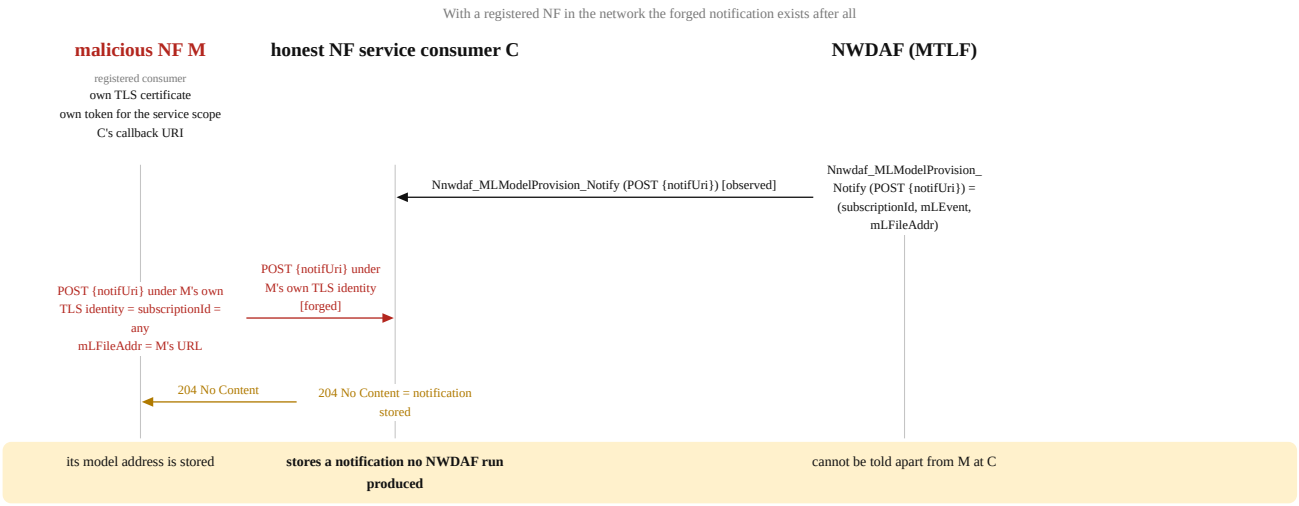
攻击者能得到什么。 消费者存储通知:它将从ML模型中获取的模型文件地址及其订阅的相关标识是恶意NF的值。 为该消费者提供示范用品被重新定位到攻击者选择的地址,它记录的示范标识不是公布的NWDAF。



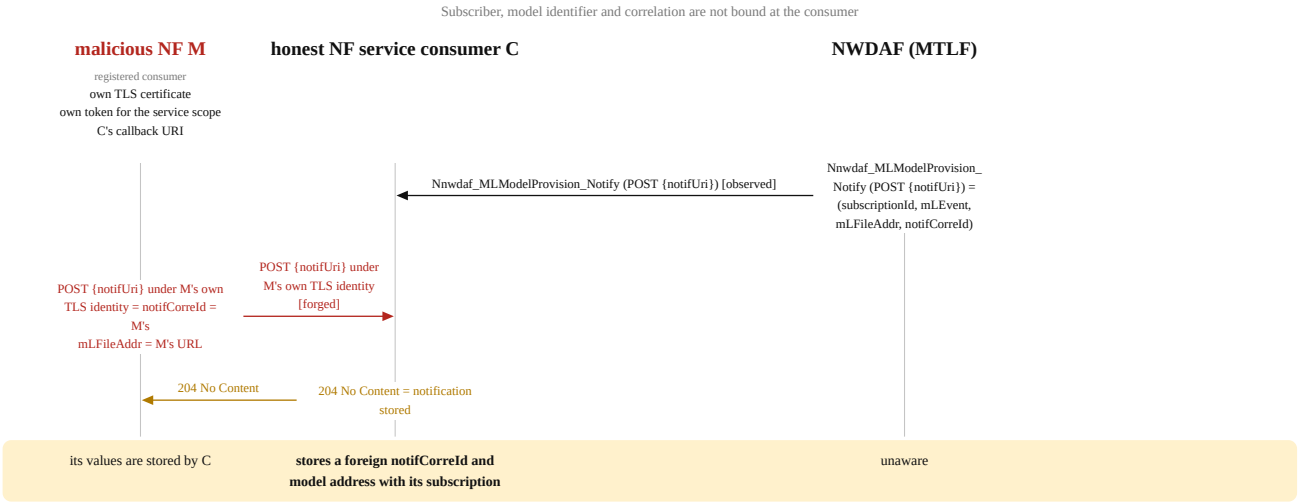
- 图2。 登记在册的NF号自带信条贴出通知C的回调URI号并C存储. 财产A03; 攻击查询 a03_nf. *



- 图3。 C存储了另一个注册的NF所选择的notifCorreId和型号地址. 财产A08; 攻击查询 a08_nf. *



- 图4。 由于网络中登记了NF,伪造的通知毕竟是存在的。 财产A03.7; 攻击查询 a03_nf。 *



- 图5。 订户、模型标识符和关联性不受消费者的约束。 财产A08.9; 攻击查询 a08_nf. *

拟议修改。 要求消费者在保存通知之前核实它是由持有其订阅的NF00个实例发送的,而且它携带的subscriptionId是其订阅地址头中退回的,并另行放弃请求。 在模型上检查时加上了这个检查:两个攻击查询在那里被核实,正常运行仍然被找到,其他记录的答案都保持不变. 一个更强的变体,在攻击者知道订阅识别器时也有帮助,它让NWDAF在授权其他操作时授权通知,而不是将通知操作留在OAuth2之外.

用 ProVerif 复核。 更改内容已输入型号副本:消费者在交存通知之前,核实它是由它同意的NWDAF号案件发出,其subscriptionId号是NWDAF号为订阅而退回的请求,但以其他方式放弃了请求。 在改变后的ProVerif型号上证明了`a03_nf`:攻击已经不可能在那里了. 协议的正常运行仍然被找到. 在记录的其他答复中,23个仍在保留,2个已更改:`a08_nf`个(A08个是攻击)现已核实; `a08_nf`(A08.9,曾遭袭击)现已核实. 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. 改型号:`records/fixes/0048-fix-notif.pv`.

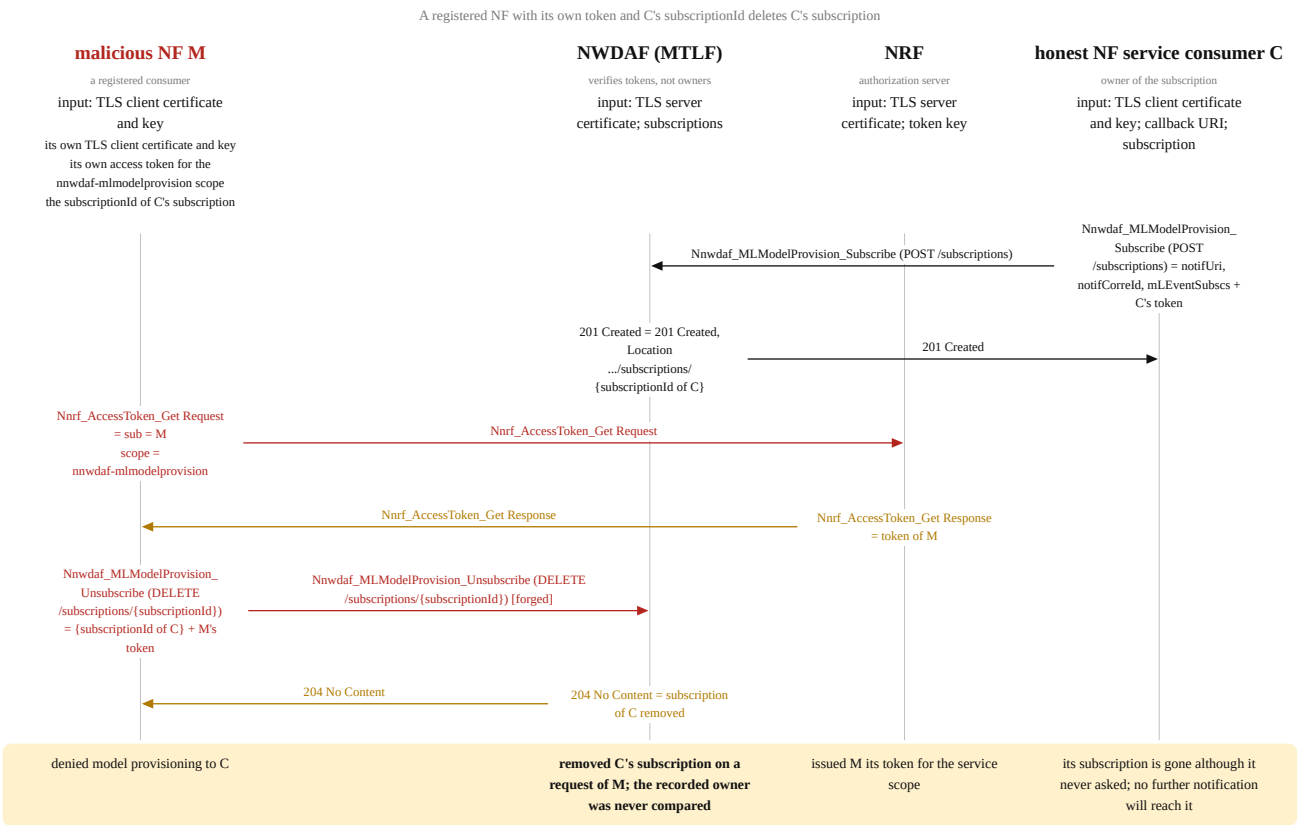
2.2 未订阅者不受订阅者约束

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-29-501:3967)
价值	中
涉及的性质	Z03, Z03.8 （见第 3 节）
原文	s0095, s0192, s0342, s0395
依据	ProVerif攻击查询`z03_other`; 图6和7

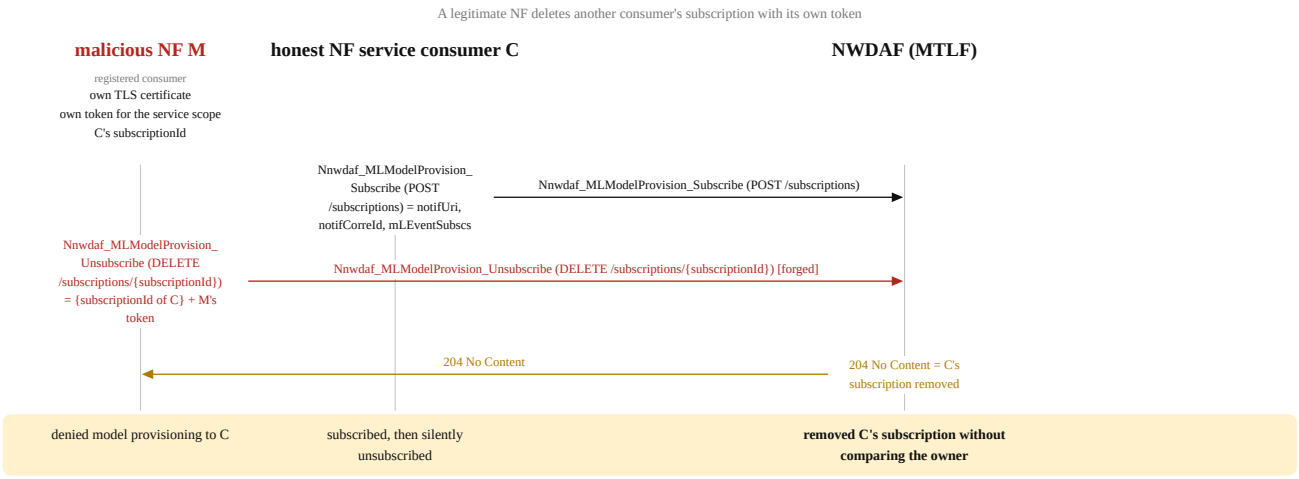
发生了什么。 Nnwdaf_MLModelProvision API 界定了一个服务级别范围,没有资源或业务范围,因此一个象征性的给予每个允许使用的消费者每一项服务业务. 未订阅者在URI号机中找到subscriptionId号机的订阅,检查了请求者的代号主题和范围,从未将请求者与创建订阅的消费者进行比较. 持有另一消费者subscriptionId的消费者因此删除了该订阅,并回答204 No Content.

攻击者需要什么。 其自己的有效登录符,用于nwdaf-mlmodel提供服务范围外加另一消费者订阅的subscriptionId,它从一个处理资源URI(间接通信的SCP,信托假设为TS 33.501 5.9.2.4)的中介机构获得,或者因为身份识别特征是不可怀疑的.

攻击者能得到什么。 消费者的订阅未经其要求而取消,因此,消费者认为订阅时,不再收到任何示范通知; 模型更新或分析的第一模型,然后就永远不会到达。 消费者对谁干的一无所知.



- 图6。 注册号为NF的自有代币,C的subscriptionId则删除C的订阅. 财产Z03; 攻击查询 z03_other. *



- 图7。 合法的NF用自己的代币删除另一个消费者的订阅. 财产Z03.8; 攻击查询 z03_other。 *

拟议修改。 要求:NWDAF,在未订阅时,比较请求中确认的订阅所有者URI由访问符号主体认证的请求人和TLS客户端证书,并在有差异时用错误答案拒绝。 使用该检查添加的模型检查: 交叉所有者删除查询在那里被核实, 正常运行仍然被找到, 其它所有记录的答案没有改变 。 或者界定订阅资源的资源范围,例如:TS29.5014.10建议赔偿额APIs其业务不能全部向每个消费者开放。

用 ProVerif复核。 该改动已纳入模型的复制本:NWDAF比较所有者所记录的用户subscriptionId请求中URI由访问符号主体认证的请求人和TLS客户端证书, 并拒绝使用错误回答, 而不是删除订阅 。 在改变的模型上ProVerif证明`z03_other`:攻击已经不可能在那里了. 协议的正常运行仍然被找到. 另一个25记录的答案保持不变。 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/0045-fix-owner.pv`.

没有为这些袭击提供数字,发现:A03.7:a08_nf,A03:a08_nf,A08.9:a03_nf,A08:a03_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
A02	**NWDAF认证消费者端点.** 每当 NWDAF（MTLF）接受一个订阅/更新/取消请求并声称对端为消费者 C 时，必须存在 C 以 NWDAF 为对端的一次真实运行。	无	成立	低	是
A03	**通知订阅者的真实性。** 每当消费者接受一条通知并声称其来自 NWDAF 且对应订阅 S 时，必须存在 NWDAF 针对同一订阅 S 的真实通知运行，且 subscriptionId、notifCorreId、notifUri、模型标识一致。	无	不成立（1 个攻击）	中	不确定
A08	**与订阅有关的通知字段。** 每当消费者接受一条通知，其中的 notifCorreId、notifUri、模型标识必须来自该消费者自己的订阅请求，且与 NWDAF 记录的订阅一致。	无	不成立（1 个攻击）	中	不确定
Z01	**核准订阅业务。** 每当 NWDAF提交一次订阅创建、更新或删除操作，必须存在 NRF为该消费者签发的、主题与消费者身份一致、观众指向 NWDAF镜片含 nnwdaf-mlmodel 规定且未过期的有效许可。	无	成立	低	是
Z03	**订阅所有权超出服务范围。** 每当 NWDAF 依据一份许可执行订阅更新或删除，该许可的 主体 必须与请求者身份一致，且被操作的 subscriptionId 属于该 主体 .	无	不成立（1 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
Z05	**交叉订阅与恶意NF隔离.** 在恶意消费者 M 控制自身凭据与自身订阅的前提下，其他消费者 C 的订阅与通知仍保持保密与认证：M 不能获得 C 的通知内容，也不能使 NWDAF 把 C 的通知发往 M 的 notifUri。	无	成立	低	是
A03.7	**正常SBA规定的通知真实性。** 在正常 SBA 端点认证加密模型下，消费者接受的通知必须对应 NWDAF 针对同一订阅的真实通知运行。	无	不成立（1 个攻击）	中	不确定
Z03.8	**交叉订阅业务的独立依据。** 每当 NWDAF 依据一份许可执行订阅更新或删除，该许可的 主体 必须与请求者身份一致，且被操作的 subscriptionId 属于该 主体 .	无	不成立（1 个攻击）	中	不确定
A08.9	**订阅者、型号编号和关联关系。** 每当消费者接受一条通知，其中的 notifCorreId、notifUri、模型标识必须来自该消费者自己的订阅请求，且与 NWDAF 记录的订阅一致。	无	不成立（1 个攻击）	中	不确定

所问之问,及分析师之答:

问题	回答	依据
Q1: 正常 SBA 下首轮通知伪造类轨迹是否消失	对网络攻击者来说是的:只有网络不能存储伪造的通知,因为存储的信息是其TLS对等端发送的. 对恶意合法NF的拒绝:注册的NF持自己的证书和信物张贴给消费者的回调URI和消费者的商店,因此一旦考虑攻击者,伪造的痕迹就会返回。	A03.7, A03, A08.9
Q2: 合法 NF 跨订阅操作是否有独立规范依据和认证前提	没有。 TS 29.552定义了整个服务的一个范围,没有资源或业务范围,其不订阅条款和TS 33.501都没有为在另一个消费者的订阅上采取行动提供依据或认证先决条件:NWDAF检查了请求者的代币并用其标识物找到资源,所有者从未被比对过. 由于没有识别资料,所有权只取决于识别资料。	Z03.8, Z03, Z01
Q3:订阅者、模型标识、 通知关联 ID 与 URL 绑定	运输将电文与发送电文的NF绑定,NWDAF将关联识别符和模型地址绑定在它持有的订阅器上; 3. 消费者一无所有 任何注册的NF的通知书都与NF的相关标识符和型号地址一同存储,因此用户,型号标识符和URL在消费者面前并不互相约束.	A08.9, A08, Z05

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:

- TLS是一个理想化的端点通道:双向键由两个NF的身份产生,没有握手,没有序列号,没有重键. 被记录的请求可以在模型中重播,没有目标基于此.
- 从通知地址下载ML型号并不是模拟的,因为任务将它排除在外; 模型地址是一种象征价值,它检查的唯一财产是它留在消费者的TLS频道内。
- 订阅店是一个单调的表格:删除是事件,记录不被删除,所以对未订阅后发生的事情没有提出询问.
- 托肯过期没有时间模型,吊销令牌根本没有模型模型; TS 33.501称撤销不予支持.
- a. 消费者的URI回调是以其注册的SBI端点为模式,文件没有说明这一点; 通知注射攻击 取决于这个选择。
- 只有直接交流是模拟的。 通过SCP或SEPP号机进行间接通信,漫游和互联,TS 33.501号机单独处理,且消费者与生产者之间没有相互认证的,则被排除在外.
- 更新订阅、即时报告和故障报告分支、403和500答案以及TS 29.552 5.4.7的错误处理的PUT业务没有模拟; 任务范围为第一轮订阅、通知和取消单一模式的订阅。
- 在NRF号和NWDAF号共用的密钥下,托肯是MACs,而不是JWS的签名; 模型代表的是生产者的检查,而不是签名计划,它没有提到计算强度。

- 拥有另一消费者subscriptionId美元的攻击者明确获得这一知识; 该模型不能显示其如何获得。

主持人记录的是什么:

- 没带对照查询的证明（附录 C）：Z05: z05_sec。 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.

A02: NWDAF认证消费者端点

每当 NWDAF（MTLF）接受一个订阅/更新/取消请求并声称对端为消费者 C 时，必须存在 C 以 NWDAF 为对端的一次真实运行。

NWDAF只接受订阅或删除它视为NF实例的TLS同行:它创建的每一订阅都带有该实例本身请求的相关标识符,而每次删除都是其中所指实例的请求. 不能要求将其看成来自另外NF, 仅针对该网络,以及另一个登记在册的NF。

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:这是相互认证和装订已要求的文件的证书(s0470、s0478); 分析证实了它,而不是找到任何新的东西。
- 在文件中说明:是的。 文件上写着:s0470,s0478
- 休息时间:TLS模拟为两个之间经认证的加密NF身份,没有握手和序列号,所以记录的请求可以在模型中重播; 2. 没有目标就靠它。 ; 标志性主题和TLS客户身份必须平等,因为TS33.50113.4.1.1.2步骤2要求; 编号NRF只是给它说话的那个例子发了个信号。 ; 订阅内容保存在只增长的表格中.
- 开放:通过SCP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,是没有模式的.
- 下一步:模拟SCP变体,看在两个端点互不认证时,装订是否仍然维持.

A03:通知用户的真实性.

每当消费者接受一条通知并声称其来自 NWDAF 且对应订阅 S 时，必须存在 NWDAF 针对同一订阅 S 的真实通知运行，且 subscriptionId、notifCorreId、notifUri、模型标识一致。

对于一个只有网络的攻击者来说,不存在伪造的通知:消费者商店是根据其自己的端点身份,由它视为对等的NF发送的。 对于持有自己的证书和象征物的注册的NF,财产失效:它向消费者的回调URI和消费者的商店发出通知,因此储存的通知不是持有订阅的NWDAF的通知。

- 结果:失败(1次攻击); 回答问题:部分; 可用备注
- 中值:TS 33.501表示,OAuth2不适用于通知业务,TS 29.552只要求消费者存储通知; 2. 既未说明通知可再由NF注射,也未要求消费者核实发送者。
- 在文件中说明:不明确。 资料来源:s0108、s0123、s0410。
- 消费者的回调URI是以其注册的SBI端点为基础的,因此为NF人所知; 这些文件没有说明它是否令人不快。 ; 消费者只进行TS 29.552规定的检查,但发件人或关系上没有这种检查; 攻击取决于这一点,TS 33.501 5.9.2.1只要求一般地验证收到的电文. ; 模型文件地址是一个固定的符号值; 。下载协议不是模拟的。
- 开放:TS 33.501 5.9.2.1是否要求消费者拒绝其持有的订阅标识符的通知.
- 下一步:请29.552名编辑说明消费者必须在通知中进行验证; 报告所检查的更改表明,将通知绑定给制作人和订阅者可以消除攻击。

A08: 通知与订阅绑定的字段

每当消费者接受一条通知，其中的 notifCorreId、notifUri、模型标识必须来自该消费者自己的订阅请求，且与 NWDAF 记录的订阅一致。

存储通知中的值正是消费者接受的信息的值,因此网络攻击者无法替代其中的任何信息. 但相关标识和模型地址与消费者商店并不挂钩:另一个注册的NF提供自己的价值,消费者储存这些价值。

- 结果:失败(1次攻击); 回答问题:部分; 可用备注
- 值介质:文档将通知相关标识符描述为可选的,并称消费者存储通知,但从未声明消费者可以得到另一方的值,也从未要求检查.
- 在文件中说明:不明确。 资料来源:s0112、s0114、s0123。
- 休息时间:URI的回调是仿照登记的SBI端点产生的。 ; 消费者不检查通知内容,因为TS 29.552没有要求它这样做。 ; 关联识别特征仅与NWDAF号相关; 没有什么能让消费者比较它。
- 开放:是否期望消费者验证notifCorreId和模型标识符.
- 下一步:与A03相同:说明消费者的支票,然后与他们一起重新运行模型.

Z01:托肯授权订阅业务.

每当 NWDAF提交一次订阅创建、更新或删除操作，必须存在 NRF为该消费者签发的、主题与消费者身份一致、观众指向 NWDAF镜片含 nnwdaf-mlmodel 规定且未过期的有效许可。

在创建或删除订阅前NWDAF以下列方式保证:NRF-发出指示,请求者就是它看到的例子TLS代号是给这个制片人的NF类型,而且其范围涵盖服务。 没有自己标志的消费者不能NWDAF行动起来。

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:支票是需要的TS 33.501 13.4.1.1.2; 分析证实了它们,而不是发现任何新的东西。
- 在文件中说明:是的。 文件上说:s0478、s0480、s0483、s0485
- 休息:过期未按时间模式进行:该模式显示对象,受众和范围检查,以及令牌与TLS身份的绑定,而非TS 33.501 13.4.1.1.2的过期支票. ; 托肯在NRF号和NWDAF号共用的密钥下模拟为MACs,而不是JWS签名,因此该模型代表的是检查而不是签名计划. ; 只有制片人NF型作为观众使用; 实例层次的受众和片面主张没有模型化。
- 开放:托肯过期且无撤销(TS 33.501状态撤销不支持)在模式之外.
- 下一步:有时间或非ce序列的模型可以询问过期或被吊销的令牌是否仍然被接受.

Z03:订阅所有权超出服务范围

每当 NWDAF 依据一份许可执行订阅更新或删除，该许可的 主体 必须与请求者身份一致，且被操作的 subscriptionId 属于该 主体 .

令牌将请求者绑定在自己的TLS个身份上,所以在另一个消费者的令牌下没有消费者的行为; 但没有什么约束订阅与它的主人。 一个拥有有效服务镜标志的消费者知道另一个消费者的订阅标识符删除了该订阅,NWDAF回答204,仿佛主人问过. 如果没有标识符,则无法删除 。

- 结果:失败(1次攻击); 回答问题:部分; 可用备注
- 价值介质:TS 29.501 4.10警告说,只有服务级别范围定义的API不得给予不当的书写或删除对不当消费者的接触,TS 29.552为整个API准确界定了一个范围; 这两份文件都没有说这API号受到影响。
- 在文件中说明:不明确。 资料来源:s0342、s0392、s0395。
- 休息:攻击需要攻击者知道另一个消费者的订阅标识符; 该模型通过一个单独的过程给出它,因为除此之外,标识符只在所有者的TLS频道内发送. ; 订阅商店是一个单调的表格:删除是事件,记录不删除,所以询问删

除后发生的事情没有属性. ; API号确定了一个服务级别范围,没有资源或业务范围,正如模型所具备的那样。

- 开放:订阅标识符在部署中是保密的还是不可知晓的; 这些文件只需要对信物和客户资格进行猜测保护。
- 下一步:在TS 29.552中澄清非订户是否必须与所有者核对,或界定资源一级的范围; 报告所检查的更改添加了所有权检查。

Z05:与恶意NF进行交叉订阅隔离.

在恶意消费者 M 控制自身凭据与自身订阅的前提下，其他消费者 C 的订阅与通知仍保持保密与认证：M 不能获得 C 的通知内容，也不能使 NWDAF 把 C 的通知发往 M 的 notifUri。

NWDAF只通知了它创建的订阅,并且只在该订阅的拥有者回调URI时才通知,因此另外NF不能让它在别处发送订阅的通知,而模型地址从不离开TLS频道在NWDAF号机与持有者之间. NF还可以做的是将自己的信息张贴到URI的回调上,这是A03和A08记录下的弱点.

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:相互认证和保护NFs,并将通知发送给召回URI订阅者,什么是TS33.5015.9.2.1财务报告和财务报告TS29.5525.4.2.4.2要求; 分析证实了这一点。
- 在文件中说明:是的。 文件上写着:s0108,s0123
- 地址:模型地址是通知中的一个象征性值; 模式文件的下载不是模拟文件。 ; 订阅表只增加,因此删除对以后通知的影响没有体现. ; 回调URI是仿照已注册的SBI端点产生的. ; 保密主张没有控制权:模型中没有揭示消费者TLS密钥的程序,加上一个会伪造其他目标的答案.
- 开放:订阅被删除后,是否继续发送通知,或被拒绝.
- 下一步:代表删除的模型会在未订阅后解决行为.

A03.7:正常情况下通知的真实性 SBA

在正常 SBA 端点认证加密模型下，消费者接受的通知必须对应 NWDAF 针对同一订阅的真实通知运行。

在端点认证运输下,外部攻击者的伪造痕迹已消失:它需要注册的NF人,并有自己的证书和自己的证物,才能使消费者商店得到从未发送的NWDAF号通知。 因此,对网络攻击者来说,这种伪造已消失,对一个有恶意的合法NF进行报复。

- 结果:失败(1次攻击); 回答问题:部分; 可用备注
- 价值介质:文件表明,通知不在OAuth2份之内,但不能让消费者储存外国通知。
- 在文件中说明:不明确。 资料来源:s0123、s0410。
- 休息时间:URI的回调假设来自注册的SBI端点. ; 消费者在保存通知时不检查发件人或订阅标识。
- 开放式:消费者欠下TS33.5015.9.2.1的验证.
- 下一步:与A03相同.

Z03.8:交叉订阅业务的独立依据.

每当 NWDAF 依据一份许可执行订阅更新或删除，该许可的 主体 必须与请求者身份一致，且被操作的 subscriptionId 属于该 主体 .

问题的第二部分有一个否定的答案,就文件的去处而言:TS 29.552定义了整个服务的一个范围,其未订阅条款对所有人没有约束力,所以删除的唯一先决条件是请求者自己的令牌和订阅标识符. 合法的NF,持有另一消费者的标识符,删除该订阅; 2. 仅由识别器持有所有权。

- 结果:失败(1次攻击); 回答问题:部分; 可用备注

- 价值介质:TS 29.501 4.10 将只允许不适当删除的API服务范围的风险点名,并要求对其进行评估; 没有说明对这API号设备的评估,也没有说明。
- 在文件中说明:不明确。 资料来源:s0192、s0095、s0395。
- 休息:身份识别知识是给予攻击者的额外能力,而不是协议揭示的东西. ; 该模型代表删除订阅,而不是删除记录的事件. ; TS 29.552 5.4.7的误差路径没有建模.
- 打开:部署中是否存在资源级范围或所有权检查。
- 下一步:将所有权检查或资源级别范围增加为TS29.552; 报告所检查的更改是第一个。

A08.9: 订户、代号模型和关联

每当消费者接受一条通知，其中的 notifCorreId、notifUri、模型标识必须来自该消费者自己的订阅请求，且与 NWDAF 记录的订阅一致。

订阅者只能通过传输与消息绑定:存储的值是发送消息的NF所写的值. 消费者中没有任何东西将模型标识符,关联标识符或回调URI绑定在自己的订阅上,所以外国通知以外国值存储,它携带的模型地址是消费者会使用的地址.

- 结果:失败(1次攻击); 回答问题:部分; 可用备注
- 价值介质:文件允许NWDAF回响notifCorreId,并提供了模型地址,但并未说明这些地址与订阅有关,也无法向消费者提供另一方的价值。
- 在文件中说明:不明确。 资料来源:s0112、s0114、s0123。
- 休息时间:URI的回调是仿照登记的SBI端点产生的。 ; 模型地址是象征性的; 该模型的下载没有建模。 ; 由于TS 29.552不需要消费者检查,消费者不检查任何物品。
- 开放:是否期望消费者将通知与其订阅进行比较。
- 下一步:与A08相同.

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		a02_sub	检查		证明:4
A03	proved		a03_end	检查	a03_nf (depends_on_ambiguity)	证实1,1次攻击
A08	proved		a08_end	检查	a08_nf (depends_on_ambiguity)	证实1,1次攻击
Z01	proved		z01_sub	检查		证明:4
Z03	proved		z03_own	检查	z03_other (depends_on_ambiguity)	证实2,1次攻击
Z05	proved		z05_dest	4中的2人		证明:4
A03.7	proved		a03_end	检查	a03_nf (depends_on_ambiguity)	证实1,1次攻击
Z03.8	proved		z03_own	检查	z03_other (depends_on_ambiguity)	证实2,1次攻击
A08.9	proved		a08_end	检查	a08_nf (depends_on_ambiguity)	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	每次订阅创建NWDAF接受带有notifCorreId用户请求的通知NF实例NWDAF视其为TLS对等点; 没有任何其他当事方以该消费者的名义订货。 攻击者只有网络	`network`	proved	a02_sub	检查
A02	每个未订阅的NWDAF处决(针对所有者或另一消费者)都是由NF实例发送的,删除请求名称是其TLS端,并带有该实例的订阅标识符。 攻击者只有网络	`network`	proved	a02_del	检查
A02	每次订阅创建NWDAF接受带有notifCorreId订阅请求的通知NF实例名称为:TLS端点, 当另一个已注册时NF拥有自己的证书和自己的服务范围标志。	`malicious_nf`	proved	a02_sub	检查
A02	每一个不订阅者NWDAF执行由NF实例 请求名称TLS,当另一个注册NF拥有自己的证书和证物; 恶意删除请求NF作为恶意请求出现NF而不是消费者。	`malicious_nf`	proved	a02_del	检查
A03	消费者存储的通知书相当于NWDAF的实际Nnwdaf_MLModelProvision_Notify00,用于同一订阅; 攻击者持有自己的NF证书,自己的服务范围的客户证书标志,并知道消费者的回调URI.	`malicious_nf`	攻击 (depends_on_ambiguity)	a03_nf	
A03	消费者视NF为它的同伴,根据自己的TLS端点身份制作了一个消费者商店的通知:仅凭网络,无法存储某些端点本身没有发送的信息。	`network`	proved	a03_end	检查
A08	消费者C存储的notifCorreId和型号地址来自C自己的订阅请求和持有该地址的NWDAF; 3. 攻击者持有自己的NF证书,它自己的服务范围标志,并且知道C的召回URI.	`malicious_nf`	攻击 (depends_on_ambiguity)	a08_nf	
A08	消费者存储的subscriptionId、notifCorreId和模型地址正是发送信件的同行的值; 网络攻击者无法替代其中任何一种。	`network`	proved	a08_end	检查

目标	主张	攻击者	回答	查询	对照
Z01	NWDAF创造的每一次订阅都附有一个访问标志,即NRF发行给同一个NF的例子:该标志主题与NWDAF所看到超过TLS的事例相吻合,其受众覆盖制作人NF类型,其范围涵盖服务范围. 攻击者只有网络	network	proved	z01_sub	检查
Z01	每个未订阅的NWDAF被执行者都有一个访问符作为后盾,即NRF被发布给同一个NF例,其主题与TLS对等,覆盖制作方的观众和覆盖服务的范围相匹配. 攻击者只有网络	network	proved	z01_del	检查
Z01	另外,当登记在册的NF00名持自己的证书和证物时,NWDAF创造的每笔订户都附有发给同一案件的NRF的证物。	malicious_nf	proved	z01_sub	检查
Z01	另外,当另一个登记在案的NF人在场时,每个未订阅的NWDAF死刑执行人都会得到发给同一案件的NRF的代号的支持,因此恶意的NF只根据自己的代号行事.	malicious_nf	proved	z01_del	检查
Z03	订阅仅由拥有该订阅的消费者删除; a 只有在攻击者已经持有subscriptionId时,才能删除另一个消费者的订阅。 攻击者只有网络	network	proved	z03_own	检查
Z03	恶意的NF,持有自己的证书和自己的服务镜标志,只有在持有subscriptionId时,才删除另一消费者的订阅; 4. 仅服务范围就使其无法获取它不知道的识别码的订阅。	malicious_nf	proved	z03_own	检查
Z03	NWDAF系未订阅者与拥有订阅权的消费者有关,而不只是允许使用该服务的消费者:持有自己代币的恶意NF,另一个消费者的subscriptionId则不得删除该订阅权.	subscription_id_known	攻击 (depends_on_ambiguity)	z03_other(控制 z03_own) (中文 (简体)).	
Z05	通知携带的型号地址从未被攻击者仅与网络接触过; 它在自己的TLS频道内到达了订阅者,而别的地方也没有。	network	proved	z05_sec	无
Z05	持有自己证书和信物的恶意NF既不获得其他消费者的订阅,也不获得其通知的内容:模型地址仅与NWDAF号机在消费者的TLS频道内运行.	malicious_nf	proved	z05_sec	无
Z05	NWDAF号只针对它创建的订阅发送通知,并且仅针对该订阅的所有人而不是所有者的回调URI号,所以网络上没有任何内容使得它向另一方发送订阅通知.	network	proved	z05_dest	检查
Z05	恶意的NF不能让NWDAF号机发送通知,要求订阅除所有者以外的URI号机位,也不能从NWDAF号机位获得另一家消费者的订阅.	malicious_nf	proved	z05_dest	检查
A03.7	消费者接受的通知相当于为同一订阅而运行的NWDAF份通知; 攻击者是注册在册的NF,拥有自己的证书和标志,知道消费者的回调URI.	malicious_nf	攻击 (depends_on_ambiguity)	a03_nf	
A03.7	在SBA终端认证运输中,一个消费者商店被其视为同行的NF以自己的身份发出通知,因此,仅凭网络就不存在伪造通知的踪迹。	network	proved	a03_end	检查
Z03.8	一个NF人没有独立的基础来更新或删除另一个消费者的订阅:除非subscriptionId已经由攻击者持有,只有其所有者才会删除订阅.	network	proved	z03_own	检查
Z03.8	持有自己的服务范围标志的合法的NF00没有依据对另一个消费者的订阅采取行动:唯一的先决条件是NWDAF支票是请求者的标志,所以所有权取决于不知道的subscriptionId。	malicious_nf	proved	z03_own	检查
Z03.8	NWDAF人不得让被允许使用该服务的消费者删除其不拥有的订阅,即使该消费者出示了自己的有效代号并命名为subscriptionId。	subscription_id_known	攻击 (depends_on_ambiguity)	z03_other(控制 z03_own) (中文 (简体)).	

目标	主张	攻击者	回答	查询	对照
A08.9	型号识别标志和通知C商店中的notifCorreId属于C自己的订阅,来源于持有它的NWDAF; 2. 攻击者是登记在册的NF人,拥有自己的证书和信物,知道C的回调URI。	`malicious_nf`	攻击 (depends_on_ambiguity)	a08_nf	
A08.9	C存储的notifCorreId、subscriptionId和型号地址正是它视为同行发送的NF的数值; 网络攻击者无法替代其中任何一种。	`network`	proved	a08_end	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-20261115T084034, 2026-11-15. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:66,校对:8 s,壁19 min,耗资0.157 USD.

ProVerif:132 证明运行,132 决定,0 未答,5 s,49 答录.

分析了什么

协议	审查ML示范条文和SBA隔离
版本	19.8.0
分析范围	复核首轮 Nnwdaf_MLModelProvision：单模型 URL订阅/通知/取消；先做规范要求的端点认证加密模型，外部攻击者不能伪造其他 TLS端点；再独立增加一个持有自己 符号的恶意消费者。禁止把全 SBI明文攻击者当正常 TLS部署；模型URL与实际下载分开，未定义的下载协议不纳入结论。
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659个编号段落(338873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	4.5	Nnwdaf_MLModelProvision 服务
主体	4.5.1	服务说明
主体	4.5.1.1	概览
主体	4.5.1.2	服务架构
主体	4.5.1.3	网络函数
主体	4.5.1.3.1	网络数据分析函数(NWDAF)
主体	4.5.1.3.2	NF 服务消费者
主体	4.5.2	服务业务
主体	4.5.2.1	导言
主体	4.5.2.2	Nnwdaf_MLModelProvision_Subscribe次服务业务
主体	4.5.2.2.1	A. 概况
主体	4.5.2.2.2	事件通知的订阅
主体	4.5.2.2.3	更新事件通知的订阅
主体	4.5.2.3	Nnwdaf_MLModelProvision_Unsubscribe次服务业务
主体	4.5.2.3.1	A. 概况
主体	4.5.2.3.2	从事件通知中取消订阅

文稿	章节	标题
主体	4.5.2.4	Nnwdaf_MLModelProvision_Notify次服务业务
主体	4.5.2.4.1	A. 概况
主体	4.5.2.4.2	关于订阅活动的通知
主体	5.4	Nnwdaf_MLModelProvision服务 API
主体	5.4.1	导言
主体	5.4.2	使用费HTTP美元
主体	5.4.2.1	A. 概况
主体	5.4.2.2	HTTP标准标题
主体	5.4.2.2.1	A. 概况
主体	5.4.2.2.2	内容类型
主体	5.4.2.3	HTTP 个自定义标题
主体	5.4.3	资源
主体	5.4.3.1	资源结构
主体	5.4.3.2	资源:NWDAF ML 示范规定订阅
主体	5.4.3.2.1	说明
主体	5.4.3.2.2	资源定义
主体	5.4.3.2.3	资源标准方法
主体	5.4.3.2.3.1	POST
主体	5.4.3.2.4	资源自定义操作
主体	5.4.3.3	资源:个人 NWDAF ML 示范规定订阅
主体	5.4.3.3.1	说明
主体	5.4.3.3.2	资源定义
主体	5.4.3.3.3	资源标准方法
主体	5.4.3.3.3.1	PUT
主体	5.4.3.3.3.2	DELETE
主体	5.4.3.3.4	资源自定义操作
主体	5.4.4	没有相关资源的自定义操作
主体	5.4.5	通知
主体	5.4.5.1	A. 概况
主体	5.4.5.2	事件通知
主体	5.4.5.2.1	说明
主体	5.4.5.2.2	操作定义
主体	5.4.6	数据模型
主体	5.4.6.1	A. 概况
主体	5.4.6.2	结构化数据类型
主体	5.4.6.2.1	导言

文稿	章节	标题
主体	5.4.6.2.2	NwdafMLModelProvSubsc型机车
主体	5.4.6.2.3	MLEventSubscription型机车
主体	5.4.6.2.4	虚拟
主体	5.4.6.2.5	NwdafMLModelProvNotif型机车
主体	5.4.6.2.6	MLEventNotif型机车
主体	5.4.6.2.7	FailureEventInfoForMLModel型机车
主体	5.4.6.2.8	MLModelAddr型机车
主体	5.4.6.2.9	虚拟
主体	5.4.6.2.10	虚拟
主体	5.4.6.2.11	MLRepEventCondition型机车
主体	5.4.6.2.12	InputDataInfo型机车
主体	5.4.6.2.13	ModelProvisionParamsExt型机车
主体	5.4.6.2.14	AdditionalMLModelInformation型机车
主体	5.4.6.2.15	MLModelAdrf型机车
主体	5.4.6.2.16	TrainInputDataInfo型机车
主体	5.4.6.2.17	InferenceDataForModelTrain型机车
主体	5.4.6.2.18	VflInfo型机车
主体	5.4.6.3	简单数据类型和计数
主体	5.4.6.3.1	导言
主体	5.4.6.3.2	简单数据类型
主体	5.4.6.3.3	编号: FailureCode
主体	5.4.6.3.4	编号: MLModelMetric
主体	5.4.6.3.5	编号: VflTrainingStatus
主体	5.4.6.3.6	编号: PositioningCase
主体	5.4.7	处理错误
主体	5.4.7.1	A. 概况
主体	5.4.7.2	协议错误
主体	5.4.7.3	应用程序错误
主体	5.4.8	特性谈判
主体	5.4.9	警卫
ts-29-501	4.10	OAuth2.0访问令牌的范围定义
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
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

文稿	章节	标题
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 Nnwdaf_MLModelProvision：单模型 URL订阅/通知/取消；先做规范要求的端点认证加密模型，外部攻击者不能伪造其他 TLS端点；再独立增加一个持有自己 符号的恶意消费者。禁止把全 SBI明文攻击者当正常 TLS部署；模型URL与实际下载分开，未定义的下载协议不纳入结论。

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	NWDAF 认证消费者端点	载有MTLF的NWDAF份申请得到保证,它接受的订阅或未订阅请求是由NF个实例发出的,它称其为同行,其身份取自TLS客户证书。	TS 33.501 13.4.1.1.2 步 2 要求制作人对照 NF 案 ID 消费者 TLS 客户证 5.9.2.1 要求消费者与制作人进行直接通信相互认证.	s0470, s0478, s0399

ID	简称	对象	文稿怎么说	出处
A03	用户的通知真实性	NF名服务消费者得到保证,它储存的通知是由持有订阅的NWDAF公司发出的,属于该订阅公司。	消费者只被告知储存接受的通知并回答204(s0123); TS 33.501 13.4.1.0说,OAuth2框架不适用于通知业务(s0410); TS 33.501 5.9.2.1要求每个NF根据协议规格和网络状态(ts-33-501:2875)验证所有收到的电文.	ts-33-501:2875, ts-33-501:7892, s0108, s0123, s0410
A08	与订阅绑定的通知字段	通知(notifCorreId、notifUri、模型标识符和模型文件地址)中消费者商店的价值是属于其订阅请求的商店。	TS 29.552 5.4.2.4.2号让NWDAF号回声notifCorreId(s0114),搭载型号地址mLFileAddr(s0112). 消费者只需存储通知并回答204(s0123),而TS 33.501 5.9.2.1则要求每NF次对网络状态(ts-33-501:2875)验证收到的电文.	s0112, s0114, s0123
Z01	订阅业务的托肯授权	NWDAF通过NRF号机发布的访问符保证,允许消费者执行订阅或不订阅操作:主题与请求实例相匹配,受众覆盖此制作人,范围覆盖服务,该信使尚未过期.	TS 29.552 5.4.9(s0339,s0340)规定OAuth2授权的接入,以NRF作为授权服务器; 2. TS 33.501 13.4.1.1.2阶 2 列出对发行者,完整性的检查,以TLS证书为准,受众,范围和到期(s0472-s0485).	s0339, s0340, s0342, s0478, s0480, s0483, s0485
Z03	超越服务范围的订阅所有权	NWDAF号涉及未订阅者为拥有订阅权的消费者,而不只是允许使用该服务的消费者.	TS 29.501 4.10说,一个具有服务范围定义的5GC API只将其所有服务业务给予所有被允许获得服务的消费者,而且必须确保它不会不适当地书面或删除对不当消费者的获取(s0392 s0395); TS 29.552 5.4.9定义了整个API的1个范围,没有资源或操作范围(s0342),未订阅条款中的任何内容对所有人的要求(s0095-s0098)都无约束力.	s0342, s0395, s0095, s0339
Z05	与恶意的NF进行交叉订阅隔离	诚实的NF服务消费者C:当同一网络的另一台NF持有自己的资质时,其订阅和通知内容仍与其同存.	TS 33.501 5.9.2.1和5.9.2.4要求在NFs之间并通过SCP进行相互认证和保密,完整性和回放保护,文件上称这为信托假设(ts-33-501:2913,ts-33-501:2921); 通知业务在OAuth2(s0410)之外,消费者只储存其收到的物品(s0123)。	s0108, s0123, s0410, s0342
A03.7	正常情况下的通知真实性 SBA	在SBA终端认证运输中,向消费者保证,它接受的通知与同一份订购的NWDAF的实际通知相符。	与A03相同:通知业务在OAuth2(s0410)以外,只告诉消费者存储通知(s0123); 直接通信需要相互认证(ts-33-501:2871)。	s0108, s0123, s0410
Z03.8	交叉订阅业务的独立依据	是否为NWDAF具有独立的规格基础和认证先决条件NF更新或删除属于另一消费者的订阅。	TS 29.501 4.10 要求在只有服务级别范围(s0392 s0395)的情况下评估API 的这种风险; TS 29.552 5.4.9 精确定义了一个服务级别范围(s0342),未订阅条款没有规定所有权检查(s0095-s0098).	s0342, s0392, s0395, s0095
A08.9	订户、代号模型和关联	存储通知中的notifCorreId,notifUri和型号标识属于该消费者自己的订阅请求,而不是另一个订阅或另一个NF的选择.	与A08号相同:NWDAF号机车可能与notifCorreId号机车(s0114号机车)和mLFileAddr号机车(s0112号机车)相呼应; 仅要求消费者存储通知(s0123); TS 33.501 5.9.2.1 需要对收到的电文进行针对网络状态的验证(ts-33-501:2875).	s0112, s0114, s0123

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 24 段，没选 374 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次安全考虑的介绍范围,以及一份单独的威胁模型文件的指针; 协议没有规定任何财产。
P003 至 P006	rfc6749:2790-2823	Z01	
P007	rfc6749:2827-2829	A02, Z01, `malicious_nf`	
P008	rfc6749:2831-2838	Z01	
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码简介; API使用没有资源拥有者的客户证书赠款。
P011	rfc6749:2859-2865	Z01, `malicious_nf`	
P012	rfc6749:2867-2868	不在范围内	关于隐含的赠款,API没有使用.
P013	rfc6749:2870-2872	Z01	
P014	rfc6749:2874-2877	Z03, `malicious_nf`	
P015	rfc6749:2879-2881	Z01	
P016 至 P033	rfc6749:2885-3003	不在范围内	更新令牌、授权代码、重定向URIs和资源拥有者的密码证书是OAuth2号赠款的一部分,API号赠款不使用。
P034	rfc6749:3013-3015	Z01	
P035	rfc6749:3017-3019	没有陈述目标	就哪些内容可在国家和范围参数内,而不是这种交换的财产提出咨询意见。
P036	rfc6749:3023-3028	A02	
P037 至 P038	rfc6749:3032-3038	Z01	
P039	rfc6749:3040-3041	不在范围内	关于打算供最终用户使用的证书; API没有最终用户证书。
P040 至 P062	rfc6749:3045-3210	不在范围内	Phishing, CSRF, 点击劫机, 代码注入, 打开重定向器和冒充在暗含的赠款中涉及基于浏览器的OAuth2客户端; 这里分析的SBI交易所没有用户代理,也没有重新定向给客户.

段落	出处	定为	不选的原因
P063 至 P213	ts-33-501:2491-2853	不在范围内	进入层,RAN、用户 -- -- 隐私和TS33.501条款5.1改为:5.8B. 与《公约》有关的事态发展UE,gNB,UDM财务报告和财务报告AUSF; 任务范围分析到 Nnwdaf_MLModelProvisionAPI子流之间NFs.
P214	ts-33-501:2859-2859	没有陈述目标	关于信任区的假设,请读者参考条款5.9.2改为:5.9.4; 它没有说明它自己的财产。
P215 至 P217	ts-33-501:2865-2869	不在范围内	约NF次服务注册和发现,而不是关于ML示范条文交易所.
P218	ts-33-501:2871-2871	A02, `malicious_nf`	
P219	ts-33-501:2873-2873	`subscription_id_known`	
P220	ts-33-501:2875-2875	A03, A08	
P221 至 P224	ts-33-501:2879-2885	Z01	
P225	ts-33-501:2887-2887	没有陈述目标	领先句子公布NRF要求名单.
P226 至 P227	ts-33-501:2889-2891	Z01	
P228 至 P234	ts-33-501:2895-2907	不在范围内	关于NEF和应用程序函数,它们不是这个API子流的当事方.
P235 至 P239	ts-33-501:2911-2919	不在范围内	相互认证和保护直接的SCP链接; 这个API的型号使用没有SCP的直通通信,这是任务修补的配置.
P240	ts-33-501:2921-2921	`subscription_id_known`	
P241	ts-33-501:2923-2923	不在范围内	关于3gpp-Sbi-Originating-Network-Id头头,它不属于模型交换的一部分.
P242 至 P314	ts-33-501:2929-3081	不在范围内	互联互通,SEPP,N32-f和IPUPS的要求涉及漫游和互联,任务对此不作规定.
P315 至 P318	ts-33-501:3085-3091	不在范围内	3gpp-Sbi-Origiating-Network-Id头的要求; 不属于认购人的财产,通知和不认购交易所.
P319 至 P337	ts-33-501:3097-3141	不在范围内	信号监测和安全配置是所分析的API分流以外的网络管理能力。

段落	出处	定为	不选的原因
P338至P369	ts-33-501:3149-3215	证明器问不了	加密与完整性算法识别符和算法谈判:一个原始的强度和算法的选择不能要求ProVerif,任务排除了范围中的计算强度.
P370至P398	ts-33-501:3219-11901	不在范围内	5G-RG、NSSAAF、N3、EAP-TLS、IAB、MBSF和MBSTF的所需经费涉及5G系统的其他部分,而不是这一API次流量。

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 36 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 6 条，没检查 30 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	不在范围内	长期的秘密是TLS端实体的私钥和NRF代键; 其机密性是TLS和OAuth2的基线(端点认证),而不是这API子流。
K02	载荷与端到端保密性	Z05	
K03	强保密／秘密值不可区分性	不适用	协议未隐藏选择的秘密值; NF个身份是公开的,两个候选价值观之间没有秘密可以区分.
K04	密钥用途、方向与会话分离	不适用	API没有建立关键等级,也没有获得它自己的密钥; 运输密钥属于TLS。
D01	消息完整性与数据来源真实性	A02, A03	
A01	对端曾参与性（ 寿命)	A02	
A04	单射一致性认证	A03	
A05	隐式密钥认证	不适用	本协议未建立密钥 。
A06	显式密钥确认	不适用	没有关键协议,因此没有要求关键确认; 通知的204答复是HTTP的确认,而不是关键确认。
A07	身份—凭据—密钥绑定	Z01, Z03	
R01	认证／挑战新鲜性	不适用	规格要求认证不存在任何质疑或新颖性机制; 标志性过期是有效限制,由Z01处理.
R02	消息级抗重放	证明器问不了	重播保护被委托给TLS运输,端点-通道模型没有序列号,因此ProVerif关于重播受保护请求的答案将是模型的动画.
R03	业务操作至多一次	证明器问不了	a. 用户的最直接语义,如重播,依赖于端点-通道模型不代表的运输属性; 规格要求无。
R04	消息接受顺序／窗口安全	不适用	API型机车没有自己的订购或验收窗口.
R05	抗降级／安全策略保持	不适用	TS 29.552条款中的特色谈判,5.4.8条款谈判了可选功能,而不是一个可以降低的安全级别或套房.
C01	前向保密性（FS）	不适用	本协议未建立会话密钥 。
C02	抗密钥泄露冒充（KCI）	不适用	此处不进行经认证的密钥交换; TLS提供,并被模拟为端点认证.
C03	已知密钥安全／泄露隔离	不适用	API没有多会键图; 每个交易所都使用其两个终点的运输证书。
C04	临时秘密／部分状态泄露韧性	不适用	API型没有可容忍渗漏的麻黄密钥或部分状态; 这些文件称没有。
C05	泄露后安全恢复（PCS）	不适用	API型机车没有重置或重置
C06	注册凭据泄露后的增强认证	不适用	使用第PAKE号或强化登记记录; 客户端认证是通过TLS证书.
C07	抗离线字典攻击	不适用	协议没有使用密码或其他低通密,因此没有线下猜测.

条目	目录里的性质	作为哪条性质检查	不检查的原因
C08	指定原语失效下的目标保持	不适用	这些文件要求当原始文件失效时不予保护; API号依赖于TLS号,OAuth2号及其给出的原始物.
Z02	委托权限不扩张	不适用	没有授权链条:SCP转发信息,但没有授权,任务排除了模式中的间接通信.
Z04	撤销与过期生效	Z01	
S01	加密 0nonce 唯一性 (中文(简体)).	不适用	API型机车本身没有使用非ce敏感AEAD型机车; TLS非斯是运输基线.
S02	重传／密钥重安装安全	不适用	API没有安装或重新安装任何密钥。
S03	抗回滚与状态单调性	不适用	API型机车没有可回滚的版本安全状态.
S04	跨阶段安全上下文一致性	不适用	在这API00个小流量中,没有登记、迁移或恢复阶段; 第A03和第A08条规定了订阅的生命周期。
S05	终止与旧状态失效	证明器问不了	这里不能要求未订阅的订阅者收到进一步通知 ProVerif : 该型号将订阅保留在单音表内,这不能代表删除.
P01	身份匿名性	不适用	NF个实例身份在SBI号上公开,并以TLS号证书携带; 这些文件声称他们不匿名。
P02	会话不可关联性	不适用	API人在整个过程中使用稳定的NF身份; 文件声称无法连接。
P03	用户／凭据存在性隐藏	不适用	API没有用户或证书存在查询; a 订阅资源由一个URI号请求人必须已经知道,作为目标Z03的识别知识。
V01	条件性进展／错误恢复	证明器问不了	进度和错误的恢复是活性问题,不能询问证明器。
V02	无非预期死锁	证明器问不了	不存在僵局是一个不能问到的活泼问题。
V03	受限资源滥用／抗放大	证明器问不了	资源滥用和扩展是费用问题,仅算出几起近似事件; 这些文件在这里没有声称什么。

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 22 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 7 项，没设的 15 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	`malicious_nf`	
S02	NWDAF	参与方	按定义全部失守	NWDAF是每个目标都具有权威性决定的政党; API号没有目标声称有消费者的保证
S03	NRF	参与方	按定义全部失守	NRF是授权服务器; API的每件授权财产都丢失了 这些文件没有要求其中任何一个 以不诚实的NRF。
S04	恶意 NF 服务消费者 M	参与方	`malicious_nf`	
S05	诚实 NF 服务消费者 C	参与方	攻击者得不到更多	持有C自身TLS密钥和信物的攻击者是已经为关于C的每一个财产设置的malicious_nf攻击者; 对于其他消费者而言,没有获得任何进一步的财产。
S06	NF 实例身份	值	攻击者得不到更多	NF个实例身份是公开的,出现在TLS证书中.
S07	TLS 端点身份	值	攻击者得不到更多	TLS端点身份是公证书身份; 2. 在没有私钥的情况下握住它给攻击者什么也没有,而握住私钥的是malicious_nf攻击者.

ID	参与方或值	类别	攻击者条件	不设的原因
S08	subscriptionId	值	`subscription_id_known`	
S09	notifCorreId	值	攻击者得不到更多	通知相关性标识符由消费者选择并反馈; 模型显示消费者没有检查它, 所以知道它没有增加 malicious_nf攻击者。
S10	notifUri	值	`malicious_nf`	
S11	modelUniqueId / mLFileAddr	值	不在范围内	模型文件地址指出一个下载,即规格留下未定义,任务排除.
S12	modelUniqueId	值	不在范围内	模型标识符属于被排除在外的下载协议.
S13	mLFileAddr	值	不在范围内	模型文件地址属于被排除在外的下载协议.
S14	OAuth2 访问令牌	值	攻击者得不到更多	制作人根据TLS客户身份对信使对象进行检查,因此没有匹配客户证书的信使无法使用; 2. 拥有自己有效标志的攻击者是malicious_nf攻击者.
S15	范围	值	攻击者得不到更多	范围为API型的公用常数.
S16	观众	值	攻击者得不到更多	观众是制作人NF型的大众.
S17	主题	值	攻击者得不到更多	主体是消费者的公众NF例身份.
S18	过期	值	攻击者得不到更多	失效期限为有效期限制; 2. 该文件指出,撤销是没有根据的,其影响是Z01主张的一部分。
S19	访问令牌	值	攻击者得不到更多	与S14相同:仅是访问符,没有消费者的TLS客户证书,就没有任何授权.
S20	C 的订阅	值	`malicious_nf`, `subscription_id_known`	
S21	C 的通知内容	值	`malicious_nf`	
S22	通知内容	值	`malicious_nf`	

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`	它是一个注册的NF服务消费者M:它持有自己的TLS客户证书和密钥,它从NRF号机为nwdaf-mlmodelproving服务范围获取了自己的访问令牌,它注册了自己的回调URI,它可以打开一个相互认证的SBI连接器,从运行开始时就可以连接到其他NF的端点.	任务范围明确指向攻击者; TS 29.501 4.10说,一个服务级的API将它的所有业务给予所有获准获得服务(s0395)的消费者,TS 29.552 5.4.9为整个API(s0342)TS 33.501 13.4.1.0 排除了OAuth2(s0410,ts-33-501:7892)和TS 33.501 5.9.2.1 只需要相互认证,所以任何注册的NF都是一个服务范围. 经认证的任何其他同位素(ts-33-501:2871)。	s0342, s0395, s0410
`subscription_id_known`	恶意的NF还知道另一个消费者订阅的subscriptionId,从处理资源URI(间接通信中的SCP,根据信托假设为TS 33.501 5.9.2.4)的中介获得,或者从规格中没有任何要求身份识别特征不能令人厌恶的事实获得.	TS 33.501 5.9.2.4 NOTE 1说,通过SCP通信的所有各方都需要信任SCP,以正确处理传递的信息(ts-33-501:2921),规格中只说明subscriptionId是一个字符串,可以识别订阅(s0192)而无需保密或不可知性要求; RFC 6749 10.10 只需要对信使和客户证进行猜测保护(rfc6749:3032).	ts-33-501:2921, rfc6749:3032, s0192

ID	network	malicious_nf	subscription_id_known
A02	成立	成立	
A03	成立	不成立	
A08	成立	不成立	
Z01	成立	成立	
Z03	成立	成立	不成立
Z05	成立	成立	
A03.7	成立	不成立	
Z03.8	成立	成立	不成立
A08.9	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：
42	A02, Z01, Z05	plain_primitives, many_sessions	这些目标仅停留在NRF-00的代号上(在主题、受众和范围方面是MAC),以终端之间认证加密为模式的运输通道上,以及任何消费者的搁置,NWDAF和NRF角色的情况是平行的。 没有算术,没有Diffie-Hellman代数,也没有跨步骤变化的值.
42	A03, A08, A03.7, A08.9	plain_primitives, many_sessions, 其他(中文(简体)).	这些目标依赖于从证书中提取的发件人身份的认证加密的运输,以及任何会议次数。 两个建模选择对他们很重要:消费者的回调URI是其注册的SBI端点(文件没有说它是否不可理解)的公用功能模型,消费者的通知接受只履行TS 29.552状态的检查,i. e. 发件人和关系上都没有
42	Z03, Z03.8	其他项目	订阅商店是一个单调的表格:一个订阅创建和向上浏览,去除不是模拟的,因此这些目标中的任何内容都不取决于一个值变化(没有计数器,序列号或替换的密钥). 他们所做的取决于一个订阅的有记录的拥有者,以及恶意的NF是否知道另一个消费者的subscriptionId,这是通过额外的攻击者流程给出的.

分析员的结语

9个目标,每个攻击者都有答案 模式上 pv(ProVerif,任何会议次数). 所有记录的27的答案仍然保留在最后的模型上; 除了Z05年的秘密指控之外 每一个攻击都有一个数字和每个证据 控制失败了

经证明成立的:SBA型运输机车和OAuth2型装订机车. 任何一方都无法再伪造TLS端点的信息(A02,以及A03/A08的端点部分),每个订阅和不订阅NWDAF执行的都有一个NRF的代币作为后盾,其主题是它所看到的连接的事例,由制作人NF型号作为观众和单一的服务范围(Z01,A02). NWDAF只通知了它创建的订阅,并且只有在该订阅者回调URI时,所以没有NF可以让它在别处发送通知,模型地址从不离开消费者的TLS频道(Z05). Z03的"身份识别器被扣"读数也被证明: 交叉所有者删除仅在攻击者获得身份识别器后才发生.

两个调查结果,都作为协议的更改加以核对。 第一,注册NF持自己的证明和信使向另一个消费者的回调发出通知URI消费者用它来储存NF'snotifCorreId和模型文件地址: 通知操作在外OAuth2消费者只需储存其所接受的东西。 将消费者的通知与生产者案例及其subscriptionId移除攻击而不失去正常运行或任何其他答案. 第二,拥有有效服务镜标志的消费者知道另一个消费者的subscriptionId删除该订阅,因为API定义一个服务范围,没有资源或操作范围,未订阅者从未将请求者与记录的所有者进行比较; 添加所有者比较会删除它。 这两件事都非常新奇,并不清楚:TS29.5014.10警告一般情况下的删除访问风险,而且两个文件都没有说明失败。

还有什么障碍:没有界限。 pv,因为没有一个目标基于一个跨步骤变化的值——订阅商店是单调的,删除不是模拟的,所以在问到一个未订阅后的行为没有任何内容. 其他简化有限度:TLS频道没有握手或序列号(因此在模型中可以重播,并且没有设定目标),回调URI假设可以从注册的SBI端点(通知注射以此为基础)中衍生出来,符号过期和吊销没有模拟,通过SCP,PUT操作的间接通信,错误路径和模型下载都在模型之外. 这两个结论不涉及代数推理,因此Tamarin+ Agent会确认而不是改变它们; 这将是解决未订阅后行为和SCP变体的工具。