NWDAF次上下文分析转移的安全分析

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))
检查的性质	10 条：8 条成立，2 条不成立（4 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

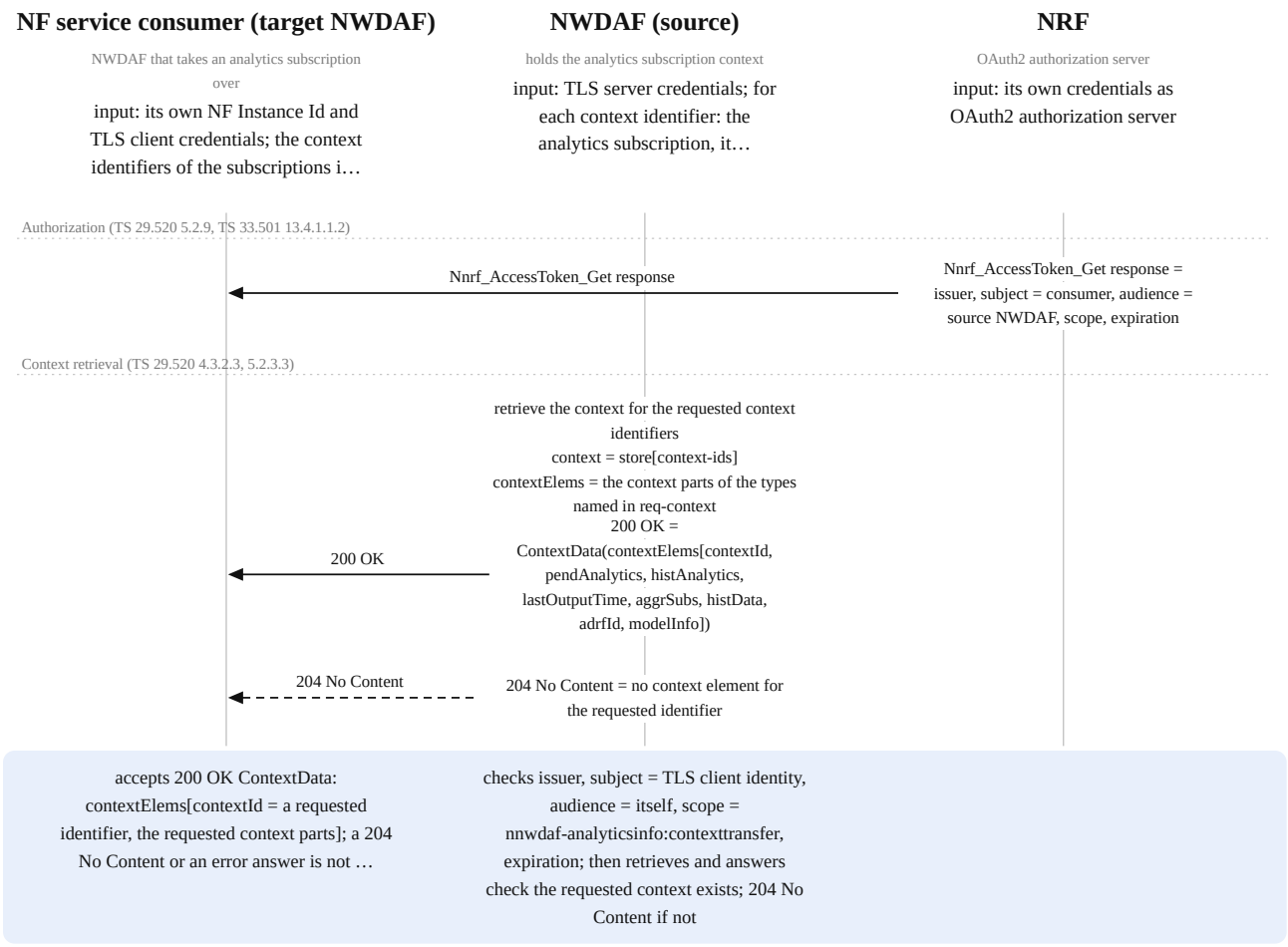
密码Nnwdaf_AnalyticsInfo_ContextTransfer服务操作允许NWDAF正在使用一个分析订阅,从中获取订阅的背景NWDAF就是这样。 消费者送一个HTTPGET日报NWDAF带有它想要的背景标识符和它希望得到的背景类型的背景资源; 编号NWDAF拥有分析订阅、其待定和历史产出分析、历史数据以及ML模式信息。 授权访问OAuth2表示NRF影响消费者的问题,以及NF实例 Id, 制作者的地址NWDAF,操作范围和到期时间。

当交换结束时,消费者持有它所命名的订阅的上下文,只有它要求的部分,而NWDAF已经根据上下文答复了200 OK,或者204没有内容时没有内容. 各方都确信,它们正在与TLS会议认证的NF对话,NWDAF确信,为这项行动向提出这项行动的一方发放了代币,但尚未过期。 双方都不能肯定,从交易所看,请求者是订阅者所属的消费者。

双方:

- **NF服务消费者(目标NWDAF)**:NWDAF,需要分析订阅。 持有:其自己的NF个实例(ID)和TLS个客户证书; 它正在接管的订阅的上下文标识符。
- **NWDAF(来源)**:持有分析订阅语境. 持有:TLS服务器证书; 对每个上下文标识符:分析订阅、其消费者、待定和历史产出分析、历史数据、ML模型信息。
- **NRF**:OAuth2 授权服务器. Holds:其作为OAuth2授权服务器的自有资质.

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。

ContextTransfer业务的操作一级授权持有:只发出一个NRF-号信使的请求,其范围是"nwdaf-analysisinfo:context transfer",其受众是这NWDAF号,其主体是经过认证的NF号信使,未到期的则送达; 4. 其他一切都得到一个错误的答案。 不持有的是一个订阅的界限:一个合法的NWDAF,它确实持有这个范围,它读取了任何订阅的解析语境,其标识名称是哪个消费者拥有的,因为NWDAF从未将请求者与订阅者的消费者进行比较. 这是一项发现,它是协议的弱点,而不是模式的弱点。 4个授权目标和4个答复处理目标在攻击者的文件名称下得到证明,每个文件都有失效的控制; 保密和具有消费者约束力的目标的所有权主张被伪造,并被记录为攻击,涉及具有消费者资格的NWDAF和持有消费者证书的一方。 结果依赖于代表TLS的模型,作为每个端点的认证加密通道,假设该令牌是不可原谅的,并将时钟解录为三个瞬间; 一个终止TLS的SCP,而由操作员配置的资源级额外范围则不在它之外。

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.

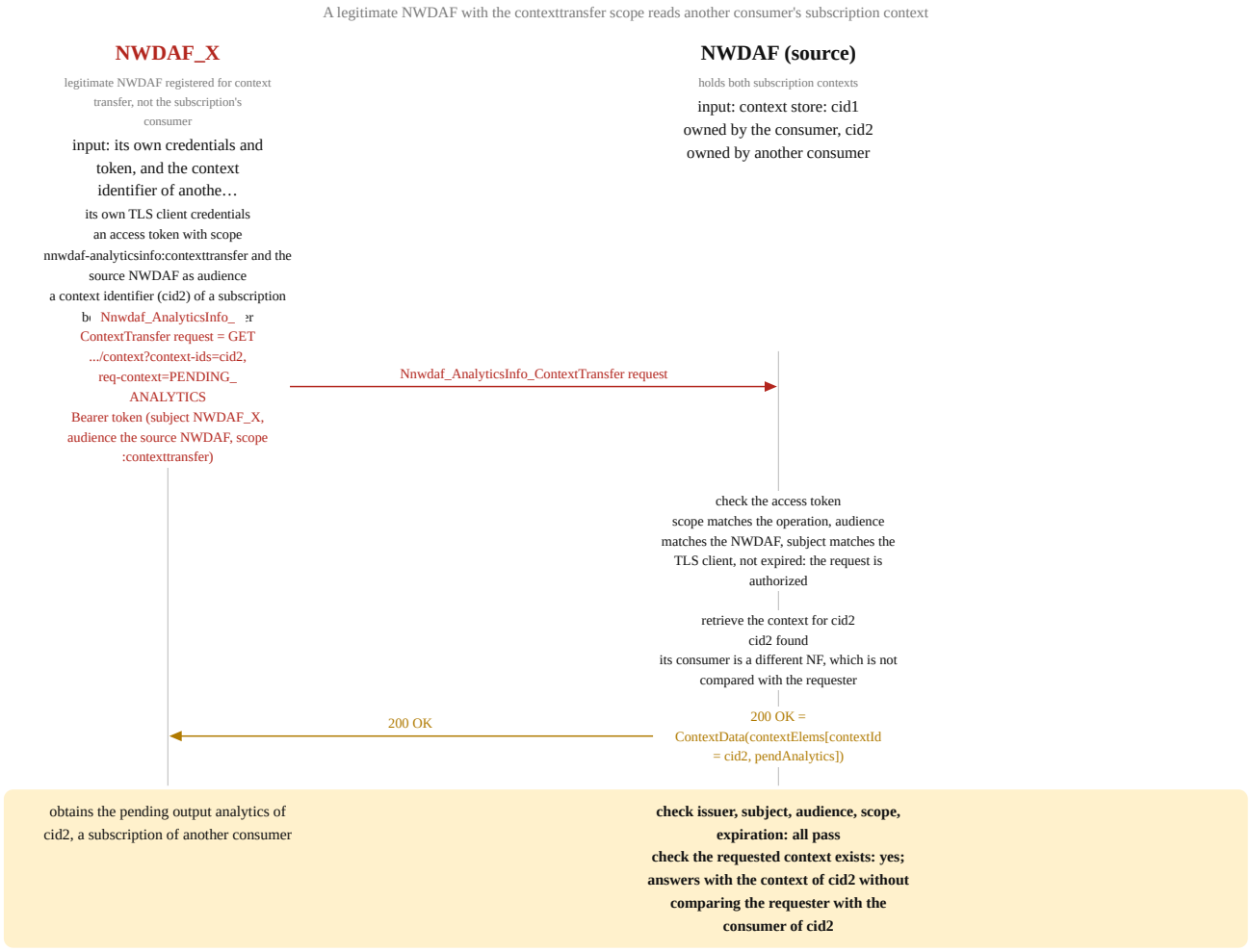
2.1 任何具有上下文传输范围的 NWDAF 可以读取另一个消费者的订阅上下文

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	K02, U01 （见第 3 节）
原文	s0009, s0010, s0097, s0222
依据	ProVerif 攻击询问 `owner,owner_x`; 图4、5、4和5

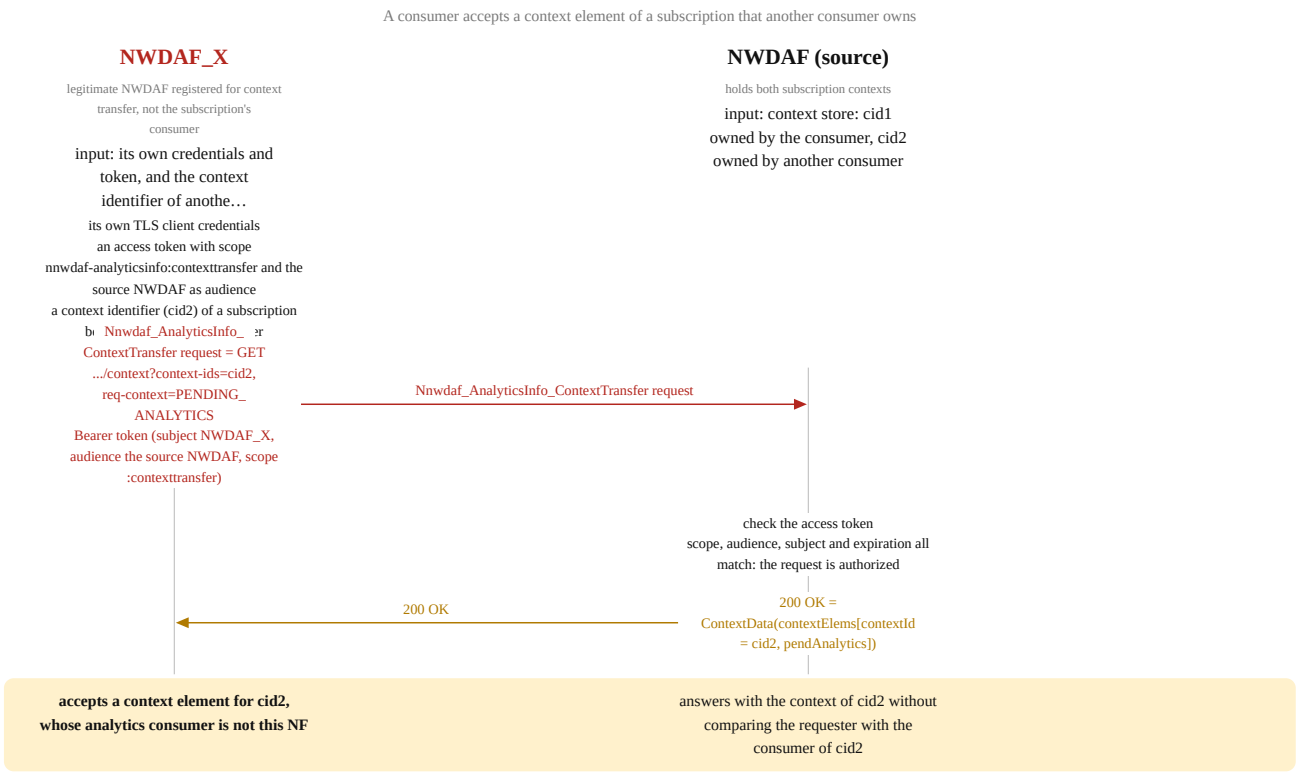
发生了什么。 来文方NWDAF授权aContextTransfer仅针对API操作范围:它检查指针的发行人、对象、受众、范围和过期日期:TS33.501要求,然后提供请求清单中任何上下文标识的上下文。 它从未将请求者与那份订阅书的分析消费者进行比较. 一个NWDAF拥有有效上下文转移符的,因此获得其名称包括其他消费者名称的每个订阅的上下文; 获得消费者证书和证物的一方也一样。

攻击者需要什么。 攻击者是注册上下文转让的合法NWDAF人,拥有自己的TLS证书和访问标志,范围为"nnwdaf-analyticsinfo:context transfer",受众为NWDAF; 任何登记在案的NWDAF都可以从NRF号机上获得这种信号。 它需要一个上下文标识符,该标识符以上下文识别符运行,并且按照TS 23.288 6. 1B. 4,在分析订阅转账请求中.

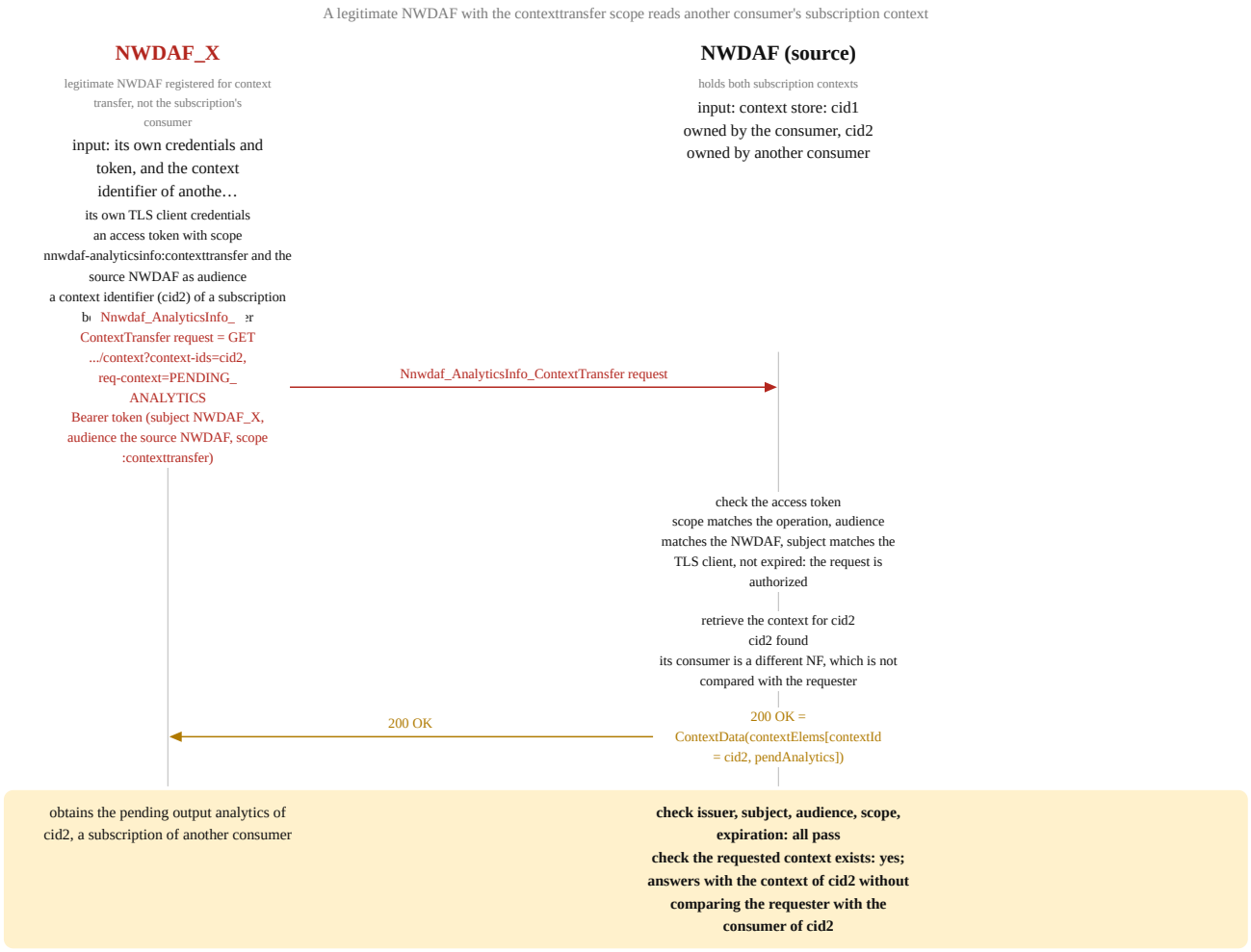
攻击者能得到什么。 攻击者阅读其他消费者订阅的待定和历史产出分析、历史数据和ML00模型信息,还可以从200 OK和204中看出不存在上下文标识符的内容。



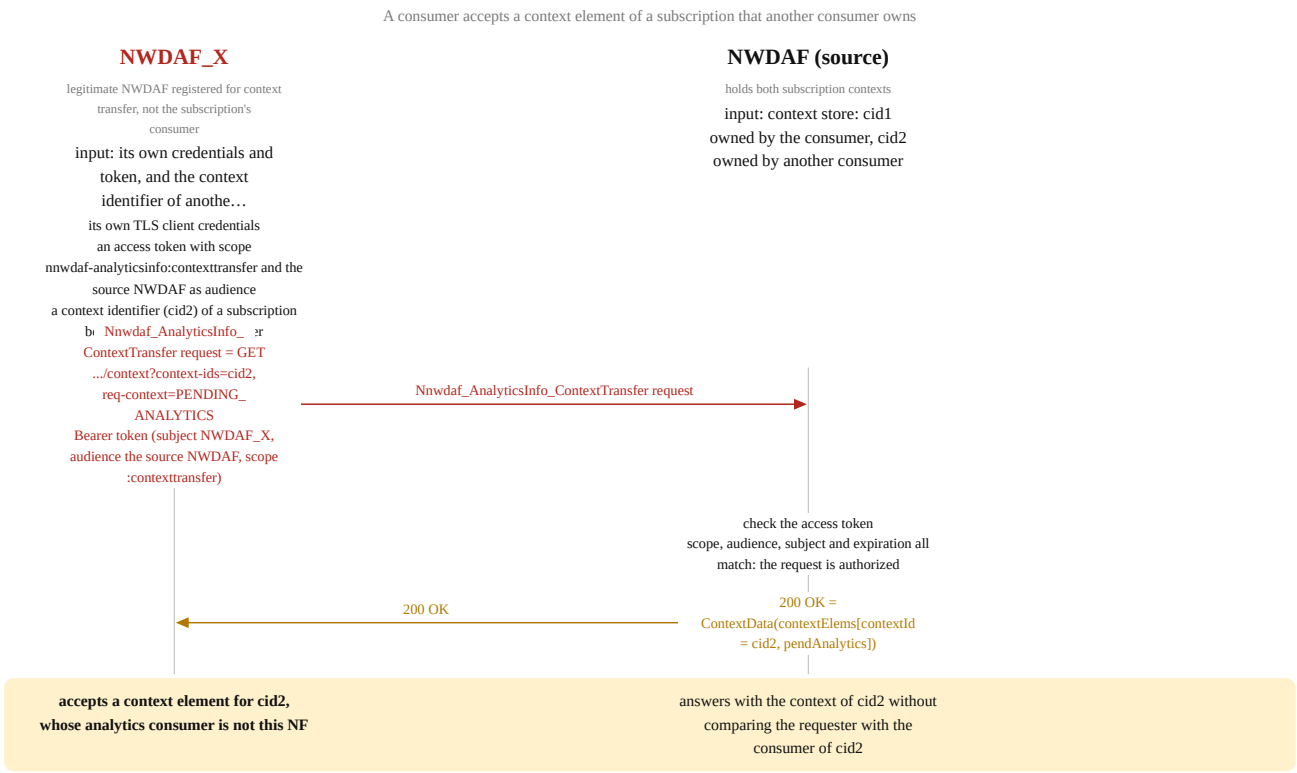
- 图4。 具有上下文转移范围的合法NWDAF读取了另一个消费者的订阅上下文。 财产K02; 攻击查询所有者 。 *



- 图5。 消费者接受另一消费者拥有的订阅的上下文要素。 财产U01; 攻击查询所有者 。 *



- 图4。 具有上下文转移范围的合法NWDAF读取了另一个消费者的订阅上下文。 财产K02; owner_x号攻击查询机主人 *



- 图5。 消费者接受另一消费者拥有的订阅的上下文要素。 财产U01; owner_x号 攻击查询所有者 *

拟议修改。 规定ContextTransfer必须获得资源级授权:NWDAF号将申请中认证的NF号与上下文标识的订阅记录分析消费者,或转让订阅时指定的消费者的NF号数据进行比较,答复403 紫禁,但两者有差异时无ContextData号。 与该比较所添加的模型核对: 所有权查询被验证,正常运行仍然被找到,其他记录的答案没有变化.

用 ProVerif 复核。 更改内容已输入型号副本:NWDAF 将上下文标识中命名的订阅者与请求中认证的NF(代号)和答复403 紫禁,两者有分歧时没有ContextData; 也就是说,TS 33.501 13.4.1.1.1的资源级授权(额外范围:消费者可以使用的资源)是ContextTransfer,而不是可选的。 在变更后的型号ProVerif上,证明了`owner`:攻击在那里已经不可能了. 协议的正常运行仍然被找到. 其他14记录的答案没有改变. 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. 改型号:`records/fixes/0046-fix-owner.pv`.

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
Z01	**内容答复需要有效授权。** 每次 NWDAF返回上下文（200OK且含 ContextData）都必须有请求方持有的、由 NRF签发且覆盖 上下文转移操作的有效授权；无有效许可的请求只能得到错误响应。	无	成立	中	否
Z03	**授权涵盖请求的上下文操作。** NWDAF返回的每个ContextElement都对应请求中列出的 上下文标识符,且该次访问的授权覆盖 上下文转移操作；为其他资源或操作取得的许可不能用于取得该上下文。	无	成立	中	否

ID	性质	假定的泄露	结果	价值	文稿是否已写
A03	**已接受上下文符合所要求的标识符。** 消费者接受（200 OK) 的 ContextData 中每个 ContextElement 的 contextId 与请求中 context-ids 一致，且对端是消费者意图通信的 NWDAF 实例。	无	成立	低	否
A08	**文稿部分采用req-context。** 响应中出现的每类上下文信息（pendAnalytics、histAnalytics、aggrSubs、histData、aggrNwdafIds、modelInfo、anaAccuInfos、modelAccuInfos）都对应请求 req 语句中指示的类型（或 req 语句缺省时的全部可用类型)。	无	成立	低	否
K02	**分析上下文不被未经授权的NFs。** ContextData 中的分析结果、历史数据与模型信息只对被授权取得该上下文的消费者可见，其他实体不能推导其内容。	无	不成立（2 个攻击）	高	不确定
U01	**Context符合请求及其所有者。** 消费者接受的每个 ContextElement的 contextId属于其请求的 上下文标识，对端为意图 NWDAF，且关联订阅的消费者为本次消费者。	无	不成立（2 个攻击）	高	不确定
Z01.7	**未经上下文转让许可,不得上下文。** 持有自身凭据但不持有覆盖该上下文 康文本转让 许可的合法 NF 不能取得该上下文。	无	成立	中	否
U02	**仅限200OK类型计算。** 消费者判定成功取得上下文时，响应为 200OK、类型与 req 语句一致、apiVersion 为 v1；204与错误响应不被当作成功。	无	成立	低	否
X01	**须受呈文NF的约束。** NWDAF号从未对一项请求作出ContextData号答复,其访问证上附有另外NF个案例的NF号; 只有在TLS会议上认证的NF号标的物上才起作用。	合法的NF通过泄漏或日志获得发给另外NF(分析消费者)的有效访问令牌,并在自己的TLS会话中呈递.	成立	中	否
X02	** 过期访问令牌被拒绝。 页:1NWDAF从来没有服务过一个ContextData答复在目前时间之前已到期的访问请求NWDAF; 此请求只得到错误答案 。	合法NF 持有其本人的证书,持有发给它的用于终止时间已过的上下文传输业务的出入证。	成立	中	否

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, X02.

所问之问,及分析师之答:

问题	回答	依据
Q1:上下文标识 与来源/目标 NWDAF 消费者身份绑定	上下文标识符与经认证的TLS会话的回答NWDAF实例和载有该实例的请求有关,因此消费者从不接受另一个标识符或另一个实例的元素; 它与消费者完全无关,因为NWDAF 服务于任何命名的标识,而不将请求者与订阅者的分析消费者进行比较,所以任何NWDAF 与操作范围读取任何订阅上下文.	A03, U01, K02
Q2: 其他合法 NF 访问该上下文的授权边界	边界仅是OAuth2范围:一个拥有自身资质但没有"nnwdaf-analysisinfo:context transfer"的NF只得到错误的答案,另一个NWDAF实例或错误主体或过期过期的标志被拒绝,但一个确实持有操作范围的NWDAF并不限于其拥有的订阅.	Z01, Z01.7, Z03, K02
Q3: 上下文类型/版本不混淆以及错误响应不作为成功传输	消费者只视其为完成的转移200OK输入apiVersionv1其部件应答其请求的上下文类型; a204没有内容或错误的答案永远不会完成一个传输,它接受的部分恰恰是请求的上下文类型.	A08, U02

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:

- 每个请求有一个上下文类型是模拟的(req-context带有单一值); 请求中不包含要求所有可用的类型,则不作模拟。
- TLS带有认证加密的模型为每对端点一个私人信道,因此该模型不代表SCP终止TLS间接通信TS33.5015.9.2.4); a 数据为:SCP阅读服务请求时,将看到上下文。
- 该出入证由NRF型机车签发; 象征性请求和NRF的授权决定不是模拟的,在没有计算论据的情况下,该标志被视为不可原谅。
- NWDAF的上下文商店是一个单调表:删除一个订阅,重新使用上下文标识符,任何上下文的生命周期都不是模型化的.
- 时钟是模型中固定的瞬间. pv和三个瞬间在边界。 pv; (中文(简体)). 代号撤销(不支持TS 33.501)和长寿代号没有建模.
- 每个政党在模式中运行一次,因此证明大约是每个政党一次上下文转移,而不是任意的届会次数.
- 307/308重定向资源答案(表5.2.3.3.3.1-3,NOTE 2)没有模型化,因此,SCP将消费者重定向到另外NWDAF例的路径已经超出了范围.
- ContextData坍塌为三部分(有待分析,历史分析,ML模型信息); 4. lastOutputTime,aggrSubs,adrfId,aggrNwdafIds和准确信息不分开.
- 可在有效范围内再次出示并再次送达一个标志(NWDAF没有使用记录); 这打破了目标属性,而是未滚动模型显示的与状态有关的行为。
- 没有提出计算主张:标志性保护的强度为TLS,任何签名都不属于模型范围。

主持人记录的是什么:

- X02的答案依赖于模型简化的操作(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.

Z01:上下文反应需要有效授权.

每次 NWDAF 返回上下文（200 OK 且含 ContextData) 都必须有请求方持有的、由 NRF 签发且覆盖 康文本转让 操作的有效授权；无有效许可的请求只能得到错误响应。

NWDAF00的答复只有在请求附有为请求签发的NRF的标语时才有上下文,其中NWDAF作为受众、上下文转移范围、NF作为主体和未到期的有效性; 每个其它请求都会得到一个错误的答案. 仅拥有网络的一方,以及持有API号机的代号但并非操作的注册号NF,均不取得上下文部分内容. 本封面中没有任何内容可供请求者阅读,这是所有权目标的主题.

- 结果:持有; 回答问题:是的; 可用备注
- 中值:它确认已按规定批准TS 29.520 5.2.9 和TS 29.500 13.3.1,这些文件已要求这样做; 结果是一种机械确认,并附有它失败的确切条件。
- 在文件中说明:否。 资料来源:s0217、s0218、s0222。
- 休息:代号为NRF型铸造的不可原谅的名词; 其密码保护没有分析。 ; TLS是每对端点的一个私人通道,因此网络攻击者既不能读,也不能注射; 终止TLS的SCP号合同不是模拟的。 ; 瞄准镜检查是每个符号一个固定字符串; NRF决定授予该范围是假定的。
- 下一步:如上所述,对主张没有开放。

Z03: 授权涵盖请求的上下文操作

NWDAF 返回的每个 ContextElement 都对应请求中列出的 文本标识符 且该次访问的授权覆盖 文本传输 操作；为其他资源或操作取得的许可不能用于取得该上下文。

消费者每ContextElement人就接受来自自己背景标识的答案,答案是发送的地址NWDAF。 仅为API范围而发行的代币,以及观众为另外NWDAF例的代币,都遭到拒绝,因此授权覆盖了这一资源上的这一操作. 范围与任何特定订阅无关。

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:证明基线所要求的范围和受众检查符合其本意; 所有权调查显示,这种机制是不够的。
- 在文件中说明:否。 资料来源:s0097、s0142、s0222。
- 休息时间:观众与制片方的NF实例ID比较; 该模型有一个生产者实例。 ; TS 33.501的资源一级额外范围是模拟没有的,因为TS 29.520没有界定这一行动。
- 开放:如TS 33.501允许,带有资源级(额外)范围的标志不是模拟的; 该模型有两个范围 TS 29.520 定义。
- 下一步:为每次订阅增加一个范围而建模,将解决标准的资源级机制是否弥合差距的问题。

A03: 接受上下文匹配请求的标识符

消费者接受（200OK）的 ContextData中每个 ContextElement的 contextId与请求中 上下文编号一致， 且对端是消费者意图通信的 NWDAF实例。

消费者只掌握了它要求的上下文识别符,由NWDAF个实例交付其TLS届会议; 用于另一个标识符的信息不符合其期望,而且网络上的一方不能置换一个。

- 结果:持有; 回答问题:是的; 可用备注
- 低值:它来自共同的TLS基线和对行动具有约束力的请求/答复; 模型的简化并不影响发现。
- 在文件中说明:否。 资料来源:s0008、s0010、s0011、s0102。
- 休息时间:每个终点TLS人,相互认证TS 33.501 13.3; 该模型除了通过NWDAF的频道外,无法联系到消费者. ; 每个请求有一个上下文标识符是模拟的,而源允许列表.
- 下一步:如上所述,对主张没有开放之处。

A08:上下文部分遵循Req-context

响应中出现的每类上下文信息（pendAnalytics histAnalytics aggrSubs histData aggrNwdafIds modelInfo anaAccuInfos modelAccuInfos) 都对应请求 req-context 中指示的类型（或 req-context 缺省时的全部可用类型)。

要求历史产出分析的消费者接受订阅的历史产出分析,而不是待决部分或模型部分,对待决类型也一样; a 部分仅针对所请求的上下文类型交付。 检查由NWDAF在选择部件时和消费者在接受部件时两次进行。

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:它确认了模拟部件规格的有条件规定规则; 警告是,八个上下文类型减少到三个。
- 在文件中说明:否。 资料来源:s0012、s0013、s0020、s0097、s0142。
- 该模型有三个上下文部分,每个请求一个请求类型; ContextType计数的8个值没有分开。 ; 没有req-context的请求,即所有类型的请求,并不是模拟的.
- 开放:盘点的其他上下文类型(aggrSubs,histData,aggrNwdafIds,准确信息)崩溃成相同的三部分.
- 下一步:将八种上下文类型分开,将涵盖整个列举。

K02: 分析上下文不被未经授权的NFs

ContextData 中的分析结果、历史数据与模型信息只对被授权取得该上下文的消费者可见， 其他实体不能推导其内容。

与网络和无操作范围的NF相比,上下文仍然关闭,但保护只是操作范围:登记用于上下文传输的NWDAF读取了它所命名的任何订阅的解析语境,无论该用户是谁拥有它。 因此,目标的承诺只存在于“授权”表示“授权”的读数中,而在“授权”表示“授权”的读数中则失败。

- 结果:失败(2次攻击); 回答问题:是的; 可用
- 价值高:它表明,在协议的模型上,这种API的授权只是操作层面的,合法的同行阅读其他消费者的分析; 这些文件没有说明这一点,也没有排除这一点。
- 在文件中说明:不明确。 资料来源:s0009、s0010、s0097、s0222。
- 续集:订阅的所有人以NF个实例为模式,按上下文录制; 来源只说上下文部分表明它与(s0011)的订阅有关。 ; NWDAF型机车的型号是准确执行TS 33.501 13.4.1.1.2步骤2的检查清单,不再使用.
- 打开(O) : 一个操作员是否要每次订阅时配置一个资源级的额外范围, 这将缩小协议文本以外的空白 。
- 下一步:一位TS 29.520的编辑会说,除了订阅的消费者之外,能否向一个NF的用户提供上下文标识,以此解决.

U01:上下文匹配请求及其所有者

消费者接受的每个 ContextElement 的 contextId 属于其请求的 康文本-代号,对端为意图 NWDAF,且关联订阅的消费者为本次消费者。

标识符和实例是受约束的:消费者只接受其要求的标识符的元素,从它所处理的NWDAF. 所有权条款失效:消费者接受的上下文要素可以涉及不同消费者拥有的订阅,因为NWDAF从未将请求者与订阅者的消费者进行比较.

- 结果:失败(2次攻击); 回答问题:部分; 可用
- 价值高:持有的两条条款是普通约束性属性,但所有权条款失败,这与消费者方面显示的保密目标相同。
- 在文件中说明:不明确。 资料来源:s0008、s0010、s0011。
- 续篇:"订阅的消费者"以每个存储的上下文1个NF个实例(Id)作为代表; TS 23.288 6 的识别码。 1B. 4不是订阅,这个概念完全没有定义.
- 打开: 源代码中允许的其他标识符的相同所有权问题(a)SUPI带分析器ID分析ID(单位:千美元)NF相关的分析,TS23.2886. 1B.4这些是分析的识别符,而不是消费者的识别符。
- 下一步:确定目标是打算订阅消费者还是指定消费者的任何NF; 来源名称。

Z01.7:未经上下文转让许可,不得上下文.

持有自身凭据但不持有覆盖该上下文 转帐 许可的合法 NF 不能取得该上下文。

合法的NF持有自己的资质,但没有上下文转移操作的令牌,不会获得上下文,只是错误的答案,所以表5.2.9-1的单独范围是阅读上下文与使用API的其余部分分开的.

- 结果:持有; 回答问题:是的; 可用
- 值介质:是操作级别授权的准确条件,也是发现显示的整个保护内容.
- 在文件中说明:否。 资料来源:s0220、s0222。
- 休息:两个瞄准镜是唯一的模拟瞄准镜; 假设NRF的配置将业务范围给予约NFs,而不给予他人。
- 下一步:如上所述,对主张没有开放之处。

U02:只有200 OK次要求的种类盘点

消费者判定成功取得上下文时， 响应为 200OK、类型与 req 语句一致、apiVersion为 v1； 204与错误响应不被当作成功。

消费者只将转帐算作完成200OK输入apiVersionv1其部件应答请求的上下文类型; a204没有内容和错误的答案是一文不值的,所以它们不能被误认为是上下文的转移。

- 结果:持有; 回答问题:是的; 可用备注
- 价值低:它确认处理规定规格的回复; 一个API的版本 没有重定向的模型不能失败。
- 在文件中说明:否。 资料来源:s0010、s0023、s0034、s0102。
- 休息:用标记和模型中的apiVersion字段来区分答案; 该模型有一个API版本,因此该版本的降级无法表示.
- 开放:307和308重定向答案不是模拟的; 与另一情况相符合的消费者不包括在内。
- 下一步:模拟两个API版本和重定向答案将测试版本主张.

X01: 受提交书约束的委托人 NF

密码NWDAF从来没有服务过一个ContextData回答一个请求,其访问符带有:NF另一种情况NF作为主题; 只有在符号主体是NF中认证的TLS载有请求的届会。

表示一个符号的NF拒绝其主体之外的其他主体:NWDAF将标的的主张与主张中认证的身份加以比较TLS因此,仅一个泄露的符号就无法访问上下文。 这是支票TS33.501添加到顶端RFC6749,这使得资源服务器无法查看向谁发放了一个令牌。

- 结果:持有; 回答问题:是的; 可用
- 值介质:它给出了被盗的令牌无用的确切条件,RFC本身说它不能提供,3GPP剖面可以提供.
- 在文件中说明:否。 资料来源:s0218。
- 休息时间:NF的TLS身份代表请求到达的终点通道。 ; 泄露的标志是仿照本来是诚实的一方; 在消费者自己的私人密钥也泄露的情况下,是拥有消费者证书的攻击者,根据定义,消费者可能做的一切都会丢失。
- 下一步:如上所述,对主张没有开放之处。

X02: 过期访问令牌被拒绝

密码NWDAF从来没有服务过一个ContextData答复在目前时间之前已到期的访问请求NWDAF; 此请求只得到错误答案 。

失效时间已经过去的访问符被拒绝:在未滚动的时钟的第三瞬间,NWDAF回答一个错误而不是上下文,而在第二瞬间发送了同样的符符,在第三瞬间发送了仍然有效的符符符. 因此,拒绝是到期核对,而不是后一时间无法到达。

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:显示过期支票工作需要TS 29.500 13.3.1, 并控制稍后的瞬间仍为有效信号; 三个瞬间是警告。
- 在文件中说明:否。 资料来源:s0217。
- 休息时间:时钟未滚动到3个瞬间,比较与台阶的瞬间; 比较的真正颗粒性不是模拟的。 ; 模拟情况是,同一NF项请求的两份请求之间到期的标志; 当信物过期时,对飞行中的请求没有任何说法。
- 开放:托肯吊销,TS 33.501表示不支持,但不能模拟:一个令牌在到期前仍然可以使用.
- 下一步: 撤销, 配置文件不支持, 需要一个单独的模型 。

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
Z01	proved		auth_secret	检查		证明:2
Z03	proved		编号	检查		证明:3
A03	proved		a03	检查		证明:2
A08	proved		a08	检查		证明:2
K02	proved		auth_secret	检查	拥有者(holds_in_source); owner_x (holds_in_source)	证实2,2次攻击
U01	proved		a03	检查	拥有者(holds_in_source); owner_x (holds_in_source)	证实1,2次攻击
Z01.7	proved		z017	检查		证明:2
U02	proved		u02	检查		证明:2
X01	proved		x01	检查		证明:1
X02	proved		x02	检查		证明1,1

以分析师对每项主张的措辞提出的主张; 每一个答案都是证明器的:

目标	主张	攻击者	回答	查询	对照
Z01	第ContextData号答案到达一个没有有效授权的一方:订阅(cid1)的分析上下文不能由拥有网络而别无其他的攻击者得出.	`network`	proved	auth_secret	检查
Z01	访问符未覆盖上下文传输操作的请求被拒绝:仅持有API范围的NF从未接受ContextData的回答,因此只能得到错误的答案. 攻击者拥有自己的NF证书和"nwdaf-analyticsinfo"的代币,没有"nwdaf-analyticsinfo:context transfer".	`nf_not_authorized`	proved	z017	检查
Z03	每ContextElement名消费者就接受一个上下文标识,这个消费者在自己要求的上下文标识中列出这个标识。	`network`	proved	编号	检查
Z03	授权必须涵盖上下文转移操作:API范围的代号只能用于获取上下文. 攻击者拥有自己的资格证书和"nwdaf-analyticsinfo"的标志,没有操作范围.	`nf_not_authorized`	proved	z017	检查
Z03	其受众为NWDAF人的一个标志不能用来获得这种背景:NF持有它从未接受ContextData的答案构成它所地址的NWDAF。	`nf_other_audience`	proved	z03_aud	检查
A03	消费者所接受的每ContextData个答复都带有其上下文标识符,并且来自其处理的NWDAF例(每个答复是200 OK,即为该标识符发送的NWDAF)。	`network`	proved	a03	检查
A03	即使对持有消费者证书和标志的一方而言,被接受为上下文的内容仍然带有所要求的上下文标识符,是发送的地址NWDAF的答案; 攻击者拥有消费者的TLS客户密钥及其访问符.	`stolen_consumer_credentials`	proved	a03	检查
A08	一个消费者要求HISTORICAL_ANALYTICSreq-context获得其订阅的历史产出分析,而不是待订部分或模型部分; 每个返回的部分都会回答请求的上下文类型。	`network`	proved	a08	检查
A08	对于持有消费者证书和证物的一方,其获得的部分仍然答复其请求的上下文类型,而不是任意的部分; 攻击者拥有消费者的TLS客户密钥和访问令牌.	`stolen_consumer_credentials`	proved	a08	检查

目标	主张	攻击者	回答	查询	对照
K02	分析背景不能由单靠网络的攻击者得出.	network	proved	auth_secret	检查
K02	拥有自己证书的NF,其符号不涵盖上下文传输操作,则获得上下文的任何部分,只是错误的答案.	nf_not_authorized	proved	z017	检查
K02	持有消费者证书和信物的一方不仅达到消费者自己的订阅环境,而且达到另一个消费者的订阅环境; 攻击者拥有消费者的TLS客户端密钥和有效上下文传输符.	stolen_consumer_credentials	攻击 (holds_in_source)	拥有者	
K02	订阅的上下文只透露给有权取得该上下文的消费者:为这NWDAF持有有效上下文转让符的另外NWDAF人获得另一个消费者的订阅上下文(其待产出分析),尽管不是该订阅的消费者,也从来不拥有它. 攻击者拥有自己的身份证明和一个有效的上下文转移符,以这NWDAF作为观众.	nf_authorized_contexttransfer	攻击 (holds_in_source)	owner_x	
U01	接受的每ContextElement人中就有一个来自消费者上下文标识的上下文标识,来自它所涉及的NWDAF例。	network	proved	a03	检查
U01	以消费者的资质和标志行事的一方接受另一消费者拥有的订阅的上下文要素; 攻击者拥有消费者的TLS客户密钥和访问令牌.	stolen_consumer_credentials	攻击 (holds_in_source)	拥有者	
U01	所接受的上下文要素涉及用户分析的消费者是该消费者:另外NWDAF00个持有有效上下文转移令牌的用户接受不同消费者拥有的上下文要素。 攻击者拥有自己的证书和这NWDAF的有效上下文转移符.	nf_authorized_contexttransfer	攻击 (holds_in_source)	owner_x	
Z01.7	NF号在没有上下文传输许可的情况下获得上下文:一个令牌没有操作范围的请求只能得到一个错误的答案.	network	proved	z017	检查
Z01.7	合法NF人拥有自己的证书,但没有上下文传输许可,就无法获得上下文信息。 攻击者拥有自己的资格证书和"nwdaf-analyticsinfo"的标志.	nf_not_authorized	proved	z017	检查
U02	在apiVersion v1中,完成的转移只是200 OK的答复,其部分答复了请求的上下文类型; a 204 没有内容或错误答案从未被视为成功转让。	network	proved	u02	检查
U02	对于持有消费者证书和证物的一方,仅在所要求的类型和版本的200OK上算作完成转让; 204和错误的答案不是成功的. 攻击者拥有消费者的TLS客户密钥和访问令牌.	stolen_consumer_credentials	proved	u02	检查
X01	以他人为对象的标志NF无法使用:NWDAF无效ContextData对不是象征性主题的请求的答复NF被证实。 攻击者持有发给消费者的有效进入证,由自己出示。TLS届会。	stolen_token	proved	x01	检查
X02	访问标志性失效时间已过的请求没有得到ContextData的答案,只是错误的答案. 攻击者拥有自己的身份证明和过期的上下文传输令牌发给它.	expired_token	proved	x02	检查
X02	访问符到期时间已过的请求没有得到ContextData的答案,只是错误的答案,此时钟已经过了到期时间. 攻击者拥有自己的身份证明和过期的上下文传输令牌发给它.	expired_token	定界(变化中的数值未滚动为 3 步)	at3_expired	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-20261114T234432, 2026-11-14. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:58,校对:20 s,壁19 min,耗资0.132 USD.

ProVerif:73 证明运行,73 决定,0 未答,8 s,25 答录.

分析了什么

协议	NWDAF 分析上下文传输
版本	19.8.0
分析范围	两个 NWDAF 直接进行单个已存在 分析学订阅上下文检索 固定 contextType 和原消费者身份; 显式区分 康特转录 与普通 08 分析结果 排除多 NWDAF 聚合、用户迁移全流程和跨 PLMN.
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263个编号段落(469990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	4.3.2.3	Nnwdaf_AnalyticsInfo_ContextTransfer次服务业务
主体	4.3.2.3.1	A. 概况
主体	4.3.2.3.2	请求和从订阅的NWDAF上下文获得
主体	5.2	Nnwdaf_AnalyticsInfo服务 API
主体	5.2.1	导言
主体	5.2.2	使用费HTTP美元
主体	5.2.2.1	A. 概况
主体	5.2.2.2	HTTP标准标题
主体	5.2.2.2.1	A. 概况
主体	5.2.2.2.2	内容类型
主体	5.2.2.3	HTTP 个自定义标题
主体	5.2.3	资源
主体	5.2.3.1	资源结构
主体	5.2.3.2	资源:NWDAF分析
主体	5.2.3.2.1	说明
主体	5.2.3.2.2	资源定义
主体	5.2.3.2.3	资源标准方法

文稿	章节	标题
主体	5.2.3.2.3.1	GET
主体	5.2.3.2.4	资源自定义操作
主体	5.2.3.3	资源:NWDAF
主体	5.2.3.3.1	说明
主体	5.2.3.3.2	资源定义
主体	5.2.3.3.3	资源标准方法
主体	5.2.3.3.3.1	GET
主体	5.2.3.3.4	资源自定义操作
主体	5.2.4	没有相关资源的自定义操作
主体	5.2.5	通知
主体	5.2.6	数据模型
主体	5.2.6.1	A. 概况
主体	5.2.6.2	结构化数据类型
主体	5.2.6.2.1	导言
主体	5.2.6.2.2	AnalyticsData型机车
主体	5.2.6.2.3	EventFilter型机车
主体	5.2.6.2.4	虚拟
主体	5.2.6.2.5	AdditionInfoAnalyticsInfoRequest型机车
主体	5.2.6.2.6	ContextData型机车
主体	5.2.6.2.7	ContextElement型机车
主体	5.2.6.2.8	ContextIdList型机车
主体	5.2.6.2.9	HistoricalData型机车
主体	5.2.6.2.10	SpecificAnalyticsSubscription型机车
主体	5.2.6.2.11	RequestedContext型机车
主体	5.2.6.2.12	SmcceInfo型机车
主体	5.2.6.2.13	SmcceUeList型机车
主体	5.2.6.2.14	SpecificDataSubscription型机车
主体	5.2.6.2.15	UserDataCongestReq型机车
主体	5.2.6.2.16	NetworkPerfReq型机车
主体	5.2.6.2.17	ResourceUsageRequPerNwPerfType型机车
主体	5.2.6.2.18	AnalyticsAccuracyInfo型机车
主体	5.2.6.2.19	GroundTruthInfo型机车
主体	5.2.6.2.20	MlModelAccuracyInfo型机车
主体	5.2.6.3	简单数据类型和计数
主体	5.2.6.3.1	导言
主体	5.2.6.3.2	简单数据类型

文稿	章节	标题
主体	5.2.6.3.3	编号: EventId
主体	5.2.6.3.4	编号: ContextType
主体	5.2.6.3.5	编号: AdrfDataType
主体	5.2.6.4	描述替代数据类型或数据类型组合的数据类型
主体	5.2.6.4.1	ProblemDetailsAnalyticsInfoRequest型机车
主体	5.2.7	处理错误
主体	5.2.7.1	A. 概况
主体	5.2.7.2	协议错误
主体	5.2.7.3	应用程序错误
主体	5.2.8	特性谈判
主体	5.2.9	警卫

协议的目的是将其定位于文件的源步骤:两个 NWDAF 直接进行单个已存在 分析器订阅上下文检索,固定 contextType 和原消费者身份； 显式区分 context transfer 与普通 08analytics results, 排除多 NWDAF 聚合、用户迁移全流程和跨 PLMN.

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
Z01	上下文响应需要有效授权	具有分析订阅背景的NWDAF保证只为请求提供ContextData(200 OK)的答案,该答复应附有NRF号为其签发的出入证,有效并涵盖ContextTransfer号业务; 任何其它请求只得到错误回复。	TS 29.520 5.2.9 说,Nnwdaf_AnalyticsInfo API号机车的进场许可与OAuth2号机车,并列出"nwdaf-analyticsinfo:context transfer"的范围为ContextTransfer; TS 29.500 13.3.1要求NF服务在允许访问前验证访问符,其过期及其访问范围.	主机:22499,主机:22507,ts-29-500:4994,s0003,s0008,s0217,s0218,s0222
Z03	授权涵盖请求的上下文操作	NWDAF保证只有在授权下才能满足请求,授权涵盖这一资源服务业务:每个返回的ContextElement回复了该请求上下文中列出的上下文标识符,为另一个范围或另一个NWDAF实例签发的令牌无法使用。	TS 29.520表5.2.9-1对ContextTransfer规定了单独的范围; 2. TS 29.500 13.3.1说,这两个范围合在一起,允许以需要具体授权的资源从事这些业务; TS 33.501 13.4.1.1.2 台阶 2要求制作人检查范围和观众.	主要内容:22507,ts-29-500:4996,ts-33-501:8032,s0097,s0142,s0145,s0154,s0222
A03	接受上下文匹配请求的标识符	NF名服务消费者(目标是NWDAF)得到保证,每接受ContextElement名服务消费者就带有它所要求的上下文标识,答复来自它处理的NWDAF例。	TS 29.520 4.3.2.3.2说,NWDAF号机为请求的上下文标识和答复检索了上下文信息,并提供了与请求中提供的上下文标识相对应的上下文信息; TS 33.501 13.3 使两个终点的相互TLS身份成为先决条件.	主机:22501,ts-33-501:8012,s0003,s0008,s0010,s0011,s0102

ID	简称	对象	文稿怎么说	出处
A08	上下文部分遵循req-context	NF名服务消费者得到保证,只有Req-context(没有req-context时所有可用的类型)所示的上下文类型才能返回上下文部分(待产出分析、历史产出分析、汇总信息、历史数据、ML模型信息、准确信息)。	TS 29.520 4.3.2.3.2和表5.2.6.2.7-1指出,每个属性"如果有这种信息,而NF服务消费者已经指明"相应的上下文类型,应提供"; 2. TS 23-288 6. 1B. 4:没有给出请求的上下文类型时,发送所有可用的类型.	ts-23-288:3005, s0012, s0013, s0015, s0016, s0019, s0020, s0097, s0142
K02	不得擅自使用分析语境NFs	上下文属于用户的分析消费者得到保证,上下文内容(待定和历史产出分析、历史数据、ML模型信息、准确信息)只向获准获得上下文的消费者披露,而且没有这种授权的网络上的NF号数据是无法获取的。	TS 29.520 5.2.9号使OAuth2号机车成为API号和TS 29.500 13.3.1号机车的出入控制装置,在允许进出前需要象征性的,到期的和范围的验证; 2. 文档中没有任何更具体的内容可以说明谁可以读取给定订阅的上下文.	主要内容:22499,ts-29-500:4994,s0010,s0012,s0013,s0016,s0020,s0217
U01	上下文匹配请求及其所有者	ContextTransfer业务的消费者得到保证,它所接受的每ContextElement项业务都带有其上下文标识,来自它所处理的NWDAF个实例,并涉及一个用户,其分析消费者就是这个消费者。	TS 29.520说,答复中包含与请求中提供的上下文识别符对应的上下文信息; TS 23-288 6. 1B. 4将操作定义为从来源NWDAF转至已接管订阅的NWDAF目标实例. 两份文件都没有说明来源NWDAF检查请求人是否拥有订阅权。	ts-23-288:2971, s0008, s0010, s0011, s0142
Z01.7	没有上下文传输许可, 没有上下文	NWDAF保证一个合法的NF,它用自己的证书认证,但其访问令牌不涵盖上下文传输操作,不会获得任何上下文信息,只是错误的答案.	TS29.520表格显示5.2.9-1将“nnwdaf-analyticsinfo”和“nnwdaf-analyticsinfo:context transfer”定义为单独的范畴,以及TS33.50113.4.1.1.2步骤2要求制作方检查范围是否与请求的服务操作匹配。	主机:22507,ts-33-501:8038,s0217,s0220,s0222
U02	只有200 OK次要求的种类清点	密码NF服务消费者得到的保证是,它只作为已完成的上下文转移处理a200OK回答带ContextData其部件匹配请求的上下文类型apiVersionv1会 议 日 程 和 议 程API,则该a204没有内容或错误答案从不被视为成功转让.	TS 29.520 4.3.2.3.2和表5.2.3.3.3.1-3界定了200 OK,ContextData和204,在没有所要求的上下文资料的情况下没有内容; 第5.2.1条对apiVersion v1作了规定。	主机:22501、s0010、s0023、s0034、s0097、s0102
X01	受呈文约束的委托人 NF	分析消费者的出入证泄露,来源为NWDAF,不得为第三批NF人提供该凭证.	TS 33.501 13.4.1.1.2 步骤 2:在直接通信案件中,生产者检查,主体主张中的NF实例ID与消费者TLS客户证书中的subjectAltName相符; 2. RFC 6749 10.3 注意到资源服务器本身没有这种手段.	ts-33-501:8028, s0218
X02	拒绝过期访问令牌	来源:NWDAF,不得接受超过有效时间的许可,以及上下文所属的分析消费者。	TS 29.500 13.3.1 需要NF 服务,以验证访问符,其过期及其访问范围; 4. TS 33.501 13.4.1.1.2 2级要求将到期时间与当前日期和时间进行核对.	ts-29-500:4994, s0217

分析者依据文稿补充的性质：X01, X02.

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 30 段，没选 368 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	说明RFC人如何为三个客户简介安排其安全考虑因素; 协议不能满足任何要求。
P003 至 P006	rfc6749:2790-2823	`stolen_consumer_credentials`	
P007 至 P010	rfc6749:2827-2850	K02, U01, `stolen_consumer_credentials`	
P011 至 P015	rfc6749:2859-2881	Z01, Z03, U02, `stolen_token`, `nf_other_audience`	
P016 至 P021	rfc6749:2885-2917	没有陈述目标	刷新令牌:本API期使用的客户证书补助金没有。
P022 至 P025	rfc6749:2921-2943	没有陈述目标	授权代码:客户证赠款未使用.
P026 至 P029	rfc6749:2947-2980	没有陈述目标	重定向 URI操纵:这个API的象征性请求不涉及重定向.
P030 至 P033	rfc6749:2984-3003	没有陈述目标	资源所有者密码证书补助:本API没有使用.
P034 至 P035	rfc6749:3013-3019	Z01, K02, `network`	
P036	rfc6749:3023-3028	A03, `network`	
P037 至 P039	rfc6749:3032-3041	证明器问不了	猜测信物和证书的概率:原始人的力量,在证明器所问之外.
P040 至 P042	rfc6749:3045-3066	不在范围内	捕捉终端用户:此交换中没有终端用户,也没有用户代理.
P043 至 P048	rfc6749:3070-3110	不在范围内	跨站点请求在重定向端点上伪造:这里没有用户代理和重定向.
P049 至 P050	rfc6749:3119-3138	不在范围内	在授权页面点击劫持:客户端证书授权中没有浏览器.
P051 至 P052	rfc6749:3142-3150	不在范围内	实施过程中的投入消毒:JSON和URI分析器的关注,而不是交换.
P053 至 P054	rfc6749:3154-3167	不在范围内	开放重定向器:这个API的服务操作不使用重定向.
P055 至 P061	rfc6749:3170-3202	没有陈述目标	滥用一个符号来冒充资源拥有者:这里既不使用隐含的流量,也不使用资源拥有者.
P062	rfc6749:3204-3210	Z03	
P063	ts-33-501:2491-2491	没有陈述目标	竞拍安全特性:本服务操作中没有特性或算法谈判.
P064 至 P072	ts-33-501:2495-2511	不在范围内	订阅认证和UE/服务网络授权; 该任务确定了两个NWDAFs之间的程序,将UE号保留在外。
P073 至 P074	ts-33-501:2515-2517	不在范围内	5GC和NG-RAN密钥要求:这些密钥都没有在这种交换中使用.

段落	出处	定为	不选的原因
P075 至 P125	ts-33-501:2523-2631	不在范围内	UE型,gNB型机车以及无线电接口上的用户隐私要求:SBI服务业务外侧分析.
P126 至 P213	ts-33-501:2637-2853	不在范围内	gNB型,ng-eNB型,SEAF型,UDM型,SIDF型,AUSF型和UDR型机车所需经费:本程序两台NWDAFs型机车以外的当事人和接口.
P214	ts-33-501:2859-2859	没有陈述目标	界定信任区,并提到5.9.2至5.9.4; 它没有说它自己必须持有的任何东西。
P215 至 P220	ts-33-501:2865-2875	Z01, Z03, A03, U02, `network`	
P221 至 P227	ts-33-501:2879-2891	Z01, Z03, `stolen_token`	
P228 至 P234	ts-33-501:2895-2907	不在范围内	NEF和应用程序功能要求:双方均不在此程序中.
P235 至 P241	ts-33-501:2911-2923	不在范围内	SCP作为中间人不在模拟部署之外:任务确定直接通信,每个端点TLS,因此终止会话的SCP不是模拟部署; 以限额表示。
P242 至 P314	ts-33-501:2929-3081	不在范围内	PLMN间互联互通,SEPP间,漫游枢纽和操作间属性:任务排除漫游和PLMN间情景.
P315 至 P318	ts-33-501:3085-3091	不在范围内	NF 互连安全要求(SEPP 附文):在模拟的PLMN直接内部程序之外。
P319 至 P327	ts-33-501:3097-3115	不在范围内	信号监测配置和流:此服务操作之外的一个操作员流程.
P328 至 P337	ts-33-501:3121-3141	没有陈述目标	安全能见度和配置性:组织要求,不是交换的属性.
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及其强度:任务排除了算法和量子后的安全性.
P370 至 P375	ts-33-501:3219-3231	不在范围内	对5G-RG和NSSAAF的要求:没有参加这一程序的当事方。
P376 至 P380	ts-33-501:6540-6548	不在范围内	N3安全:此程序中没有使用飞机.
P381 至 P394	ts-33-501:9656-10917	不在范围内	EAP-TLS订阅标识隐私和IAB要求:其他程序.
P395 至 P396	ts-33-501:11439-11443	不在范围内	MBSF和MBSTF要求:没有参加这一程序的当事方。

段落	出处	定为	不选的原因
P397 至 P398	ts-33-501:11899-11901	不在范围内	NEF安全要求:本程序中无NEF.

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 26 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 14 项，没设的 12 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	`stolen_consumer_credentials`	
S02	NWDAF	参与方	按定义全部失守	NWDAF号拥有整个上下文商店; 控制它给出每个订阅的上下文,文档对持有数据的一方不要求保密.
S03	NRF	参与方	按定义全部失守	如果NRF被控制,任何主题,范围和观众都可以铸造代币,因此,这API的授权财产不能在它下要求.
S04	其他合法 NF	参与方	`nf_not_authorized`, `nf_authorized_contexttransfer`, `nf_other_audience`, `stolen_token`, `expired_token`	
S05	外部网络攻击者	参与方	攻击者得不到更多	本条目是攻击者与网络本身,每个财产都根据这一基线得到答复; 它没有增加任何能力 超越网络。
S06	OAuth2 访问令牌	值	`stolen_token`, `stolen_consumer_credentials`	
S07	范围 nnwdaf-analystics 信息:context transfer	值	`nf_authorized_contexttransfer`	
S08	分析订阅 上下文	值	`nf_authorized_contexttransfer`	
S09	上下文标识符	值	攻击者得不到更多	上下文标识符由请求者以上下文标识提供; 2. 拥有它本身就无济于事
S10	OAuth2令牌 的 瞄准镜与受众	值	`nf_other_audience`, `stolen_token`	
S11	ContextData/ContextElement	值	`nf_authorized_contexttransfer`	
S12	上下文编号	值	攻击者得不到更多	上下文标识是一个由消费者选择的请求查询参数; 它不会保护任何东西。
S13	req-context 类型 (韩语)	值	攻击者得不到更多	req-context是消费者选择的请求查询参数; 持有它没有任何好处。
S14	ContextData	值	`nf_authorized_contexttransfer`	
S15	req-context / ContextType (中文(简体)).	值	攻击者得不到更多	ContextType值是该规格的公开列举.
S16	ContextElement 各属性	值	`nf_authorized_contexttransfer`	
S17	pendAnalytics/histAnalytics	值	`nf_authorized_contexttransfer`	

ID	参与方或值	类别	攻击者条件	不设的原因
S18	histData	值	`nf_authorized_contexttransfer`	
S19	modelInfo	值	`nf_authorized_contexttransfer`	
S20	anaAccuInfos/modelAccuInfos	值	`nf_authorized_contexttransfer`	
S21	NWDAF 实例身份	值	按定义全部失守	如果攻击者持有NWDAF个案例的证书,就是那个案例,它提供的所有财产都丢失了; 实例身份本身在SBI上是公开的。
S22	消费者身份	值	攻击者得不到更多	消费者的NF实例在SBI上是公开的; 它只允许冒充客户资格, 而在攻击者名单上。
S23	OAuth2令牌 与 镜	值	`stolen_token`, `nf_not_authorized`	
S24	ContextType	值	攻击者得不到更多	ContextType计数器在规格上是公开的.
S25	apiVersion	值	攻击者得不到更多	apiVersion弦是每个请求URI的一部分,并且是公开的.
S26	204 无内容 与错误响应	值	攻击者得不到更多	错误或204的答案没有上下文数据; 消费者的规则是,只有200的OK和ContextData的计数,成功的目标要求这样做。

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		
`nf_not_authorized`	一个合法的NF,拥有自己的TLS客户资格,注册于NRF,持有一个访问令牌,范围只有"nwdaf-analyticsinfo",没有"nwdaf-analyticsinfo:context transfer".	TS 29.520 表5.2.9-1 将API范围与上下文转移范围相分离,TS 33.501 13.4.1.1.2只有NRF的发行量为消费者授权的范围.	主机:22507,s0222
`nf_authorized_contexttransfer`	一个合法的NWDAF,拥有自己的证书和一个有效的访问符,其范围是"nwdaf-analyticsinfo:context transfer",其受众是制作的NWDAF,但并不是它要求的订阅的分析性消费者; 它选择上下文标识符和请求的上下文类型本身。	TS 29.520 将操作范围确定为仅API级,TS 29.500 13.3.1 使额外的资源级操作范围具有可选性,因此任何NWDAF 注册用于操作的操作都持有用于任何上下文标识的这种标志; TS 33.501 13.4.1.1.2 阶 2 检查请求人与没有资源拥有者.	ts-29-500:4996, s0222, s0097
`nf_other_audience`	一个合法的NF 持有有效出入证,其上下文传输范围与它所处理的NWDAF例不同。	TS 33.501 13.4.1.1.2 台阶 2 要求制作人对照自己的身份来检查观众的诉求,这预示着一个制作人可以向另一个制作人展示的标志.	ts-33-501:8032, s0222
`stolen_token`	合法的NF通过泄漏或日志获得发给另外NF(分析消费者)的有效访问令牌,并在自己的TLS会话中呈递.	TS33.50113.4.1.1.2步骤2要求制作方将符号标的与subjectAltName一、导 言1 - 2 3NF'sTLS客户证书,它预先假定不是当事人的一方出示的标志。	ts-33-501:8028, s0218
`stolen_consumer_credentials`	一方获得了TLS客户私钥和NF实例的分析性消费者,因此可以认证为该消费者,对NRF和来源的NWDAF。	RFC 6749 10.1 和 10.2:客户必须对其客户资格保密,持有他人客户资格的恶意客户可以冒充; 2. 在SBI上 客户证是TLS客户私钥	rfc6749:2827, s0218

攻击者	持有什么	依据	出处
expired_token	合法NF 持有其本人的证书,持有发给它的用于终止时间已过的上下文传输业务的出入证。	TS 29.500 13.3.1和TS 33.501 13.4.1.1.2 台阶 2 要求制作方对照当前日期和时间检查到期时间.	ts-29-500:4994, s0217

ID	network	nf_not_authorized	nf_authorized_contexttransfer	nf_other_audience	stolen_token	stolen_consumer_credentials	expired_token
Z01	成立	成立					
Z03	成立	成立		成立			
A03	成立					成立	
A08	成立					成立	
K02	成立	成立	不成立			不成立	
U01	成立		不成立			不成立	
Z01.7	成立	成立					
U02	成立					成立	
X01					成立		
X02							成立

关于证明和模型的说明

- X02: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。

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
进入证的到期时间(到期主张)	NRF 发布过期时间; NF服务消费者持有其标志; NWDAF号比对它	在稍后的服务请求之前,从NRF申请新的访问令牌; 已经发行的符号保持其值	每ContextTransfer项请求,NWDAF号请求在允许访问前将其与当前日期和时间进行比较	s0217, s0218, s0222
NWDAF的当前日期和时间	NWDAF号公路	它在步间和会间实时推进	与每次请求中 令状的过期时间相对应	s0217
上下文存储:上下文标识符、所有者(分析消费者),待定和历史产出分析,ML模型信息	NWDAF号公路	只有在分析订阅书被创建或删除时,两者都不属于这一程序范围; 上下文转移请求不更改它	查看每个已送达请求的上下文标识符	s0009, s0023, s0086

模式	结果	目标	显示于 ProVerif	步骤
重播(E)	候选人		是: ProVerif 伪造 `at2_same_token` 页:1	NF型机车为上下文传输操作获得一个令牌,有效期至即时2(TS 29.520 5.2.9 s0217). 它发送GET。 . . /context 上下文标识符 cid1 与该标识符并发(s0008,s0009). / 2瞬间,它再次以同样方式发出同样的请求,并再次得到服务; NWDAF型机车没有能够使第二型机车的用途区分开来.
update_before_check	没有找到			NWDAF在请求中不更新值:它读取商店和答案. 检查前没有改变
no_rollback_on_failure	没有找到			一个被拒绝的请求(过期的令牌,错误的范围,错误的受众,错误的主题)在NWDAF中没有任何改变,一个废弃的运行离开了商店原样.
race_between_sessions	没有找到			两次运行的值不会改变其中任何一项; 该商店只读取此程序。
distinguishable_failure	没有找到			答案确实不同(一个被拒绝的令牌错误的答案,204 不包含上下文的标识符内容),但204是在检查通过后才发送的,所以只有已经授权操作的请求者才会看到差异,它无论如何都可以读取上下文.
repeat_one_time_action	没有找到			没有安装密钥,在这一程序中也不存在一次性步骤; GET型机车具有特异性,店铺不因该型机车而改变.
脱同步	没有找到			双方没有保持和调和的一对价值观; 这只比作NWDAF的时钟
wrap_or_window	没有找到			到期日检查对于未来到期时间可能有多远没有上限,也没有验收窗口; 2. 时钟未滚动到三个瞬间,内部没有包裹。 每一次不滚动的瞬间,都会接受一个过期很久的代币,这是来源要求的,所以没有记录为候选人.

分析师给目标取了什么名字?

步骤	目标	特性	原因：
37	Z01, Z03, A03, A08, K02, U01, Z01.7, U02, X01	plain_primitives, many_sessions	该代币的模型是仅由NRF人铸造的不可原谅的名词,而运输则作为每个端点的认证加密通道,因此只使用平原原始(没有代数); 其属性大约为每期2,NWDAFs次传输,和模型。 pv运行每方运行一次,所以证明覆盖了这些运行而不是任意的数量.
37	X02	changing_state	拒绝发放过期访问证的要求,取决于该证件的到期时间与NWDAF的当前时间,该证件在台阶和会话之间垫付; 型号。 pv比较一个固定的瞬间,所以属性需要没有捆绑的时钟. 页:1

分析员的结语

在ProVerif中模拟了Nnwdaf_AnalyticsInfo_ContextTransfer检索(TS 29.520 4.3.2.3/5.2.3.3),授权每TS 29.500 13.3.1和TS 33.501 13.4.1.1.2),每个端点有TLS作为经认证的加密通道,访问令牌作为不可原谅的术语,携带对象,受众,范围和到期.

每个目标都有一个答案, 逐项要求, 在每个攻击者为它设定。 证明(在每一种情况下都有失败的控制权):ContextData答案需要此操作的有效符号NWDAF(Z01,Z01.7,Z03); 所接受的元素带有请求的地址上下文标识符NWDAF(A03,U01第1条); 部分遵循req-context(A08); 仅限 a200OK输入v1算作转让(E)U02); 签发给他人的令牌NF被拒绝(X01); 拒绝过期的令牌(X02,同样以时钟为界的平面,未滚动到三个定界的瞬间. pv,即刻发出同样的信号2并立即拒绝3).

伪造并报告为一项发现:订阅的界限。 这里授权的仅是API操作范围,因此合法持有"nwdaf-analyticsinfo:context transfer"的NWDAF读了任何订阅的上下文,其标识名称由消费者所有(K02和U01所有权主张,lemma所有者和owner_x,holds_in_source判决). 该建议——将经认证的请求者与订阅者的消费者进行比较,并回答403,否则——在一份模型副本中被检查:攻击查询得到核实,正常运行和所有其他记录的答案没有变化. 小说尚不清楚,因为TS 33.501提供了可选资源级的附加范围,TS 29.520名称完全没有检查.

还有什么障碍:终止TLS的SCP(TS 33.501 5.9.2.4)不在模型之外,所以阅读请求的SCP会看到上下文; a. 由运算符配置的资源级额外范围,没有Req-context(所有类型),没有模拟307/308重定向路径和撤销符号; 每方运行一次,所以证明 大约每方一次转移。 在有效范围内重放一个令牌是可能的,并且不突破任何目标.