ML次审查模式监测与SBA次隔离的安全分析

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	15 条：8 条成立，7 条不成立（8 个攻击）
发现	1；另在附录 B 复现已知结论： 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 B：复现的已知结论
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

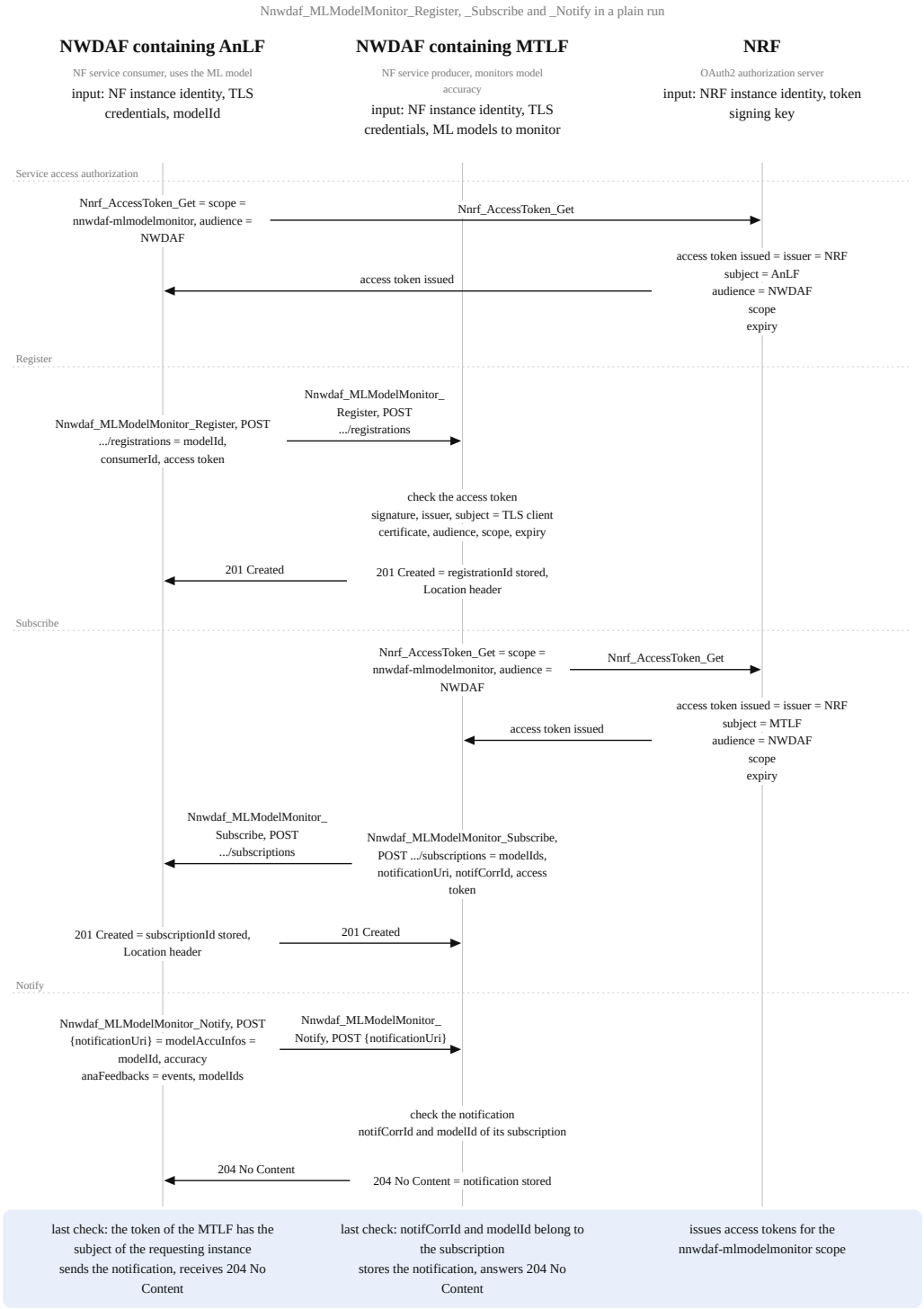
Nnwdaf_MLModelMonitor服务是5G核心接口,其中一个网络数据分析函数实例说明了它使用的ML模型的运作情况。 载有AnLF的个案采用该模型,与载有MTLF的个案进行登记,随后报告所测量的准确性和分析反馈;载有MTLF个案例的个案赞同这些报告并收到这些报告。 API号机获准使用NRF号机签发的OAuth2号机进入证,并请求通过相互认证的TLS号机进行旅行。

当交换结束时,消费者确信接受其注册和订阅的生产者是代号中指定的例子,每一次接受都属于自己的一个请求,并且它得到的标识是自己的. 制作人确信,它收到的通知载有它创建的订阅的关联标识符和模型标识符,这些标识符是该订阅的制作人在其TLS届会议期间发出的,没有其他NF个实例获得其注册或订阅标识符。

双方:

- **NWDAF 含AnLF**:NF 服务消费者,使用ML型号. 持有:NF个案例身份,TLS个证书,modelId.
- **NWDAF 含MTLF**:NF 服务生产商,显示器型号精度. 持有:NF例身份,TLS合格证,ML型号用于监控.
- **NRF**:OAuth2 授权服务器. 持有:NRF个实例身份,标志签名密钥.

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。 1 的结果是,文件已说明不计算,并载于附录B。

协议给出了反对网络和恶意NF的意向,但有一个例外:注册的consumerId不受经认证的消费者的约束. 所有其他故障要么在来源中说明,要么在模型的一件文物中说明。 在15个目标中,14个目标得到答复,每个攻击者都得到答复; 第十五,请求创建,在它的标识-注入读物中被证明,在它的回放读物中仍然是一个模型文物. 通知路径仅由TLS号保护,消息来源指出,因此它属于来源也指出的已受损的SCP号。 结果在于简化的TLS号,没有握手,以及仿照其主张的签名的出入标志。

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.

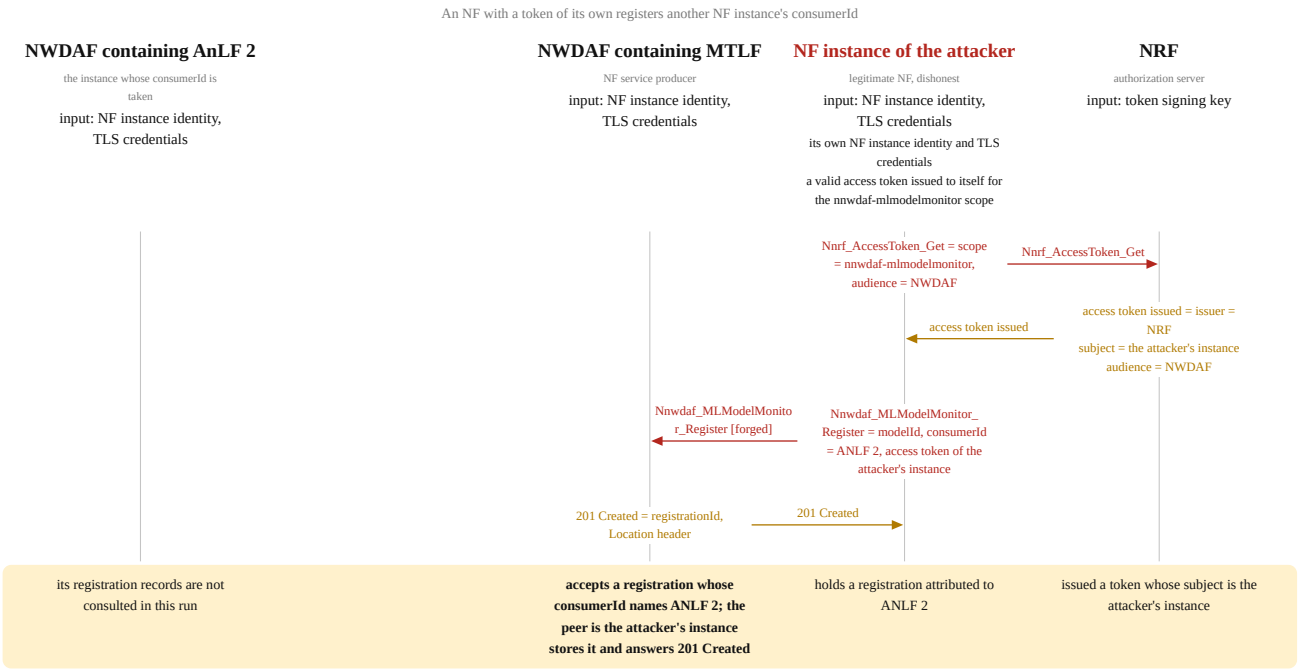
2.1 NF号案例可以登记 NF号案例的consumerId号案例

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	中
涉及的性质	A07, Z03, U03 （见第 3 节）
原文	s0040, s0041, s0042, s0480, s0347
依据	ProVerif攻击查询`a07_body_nf`; 图2、3和4

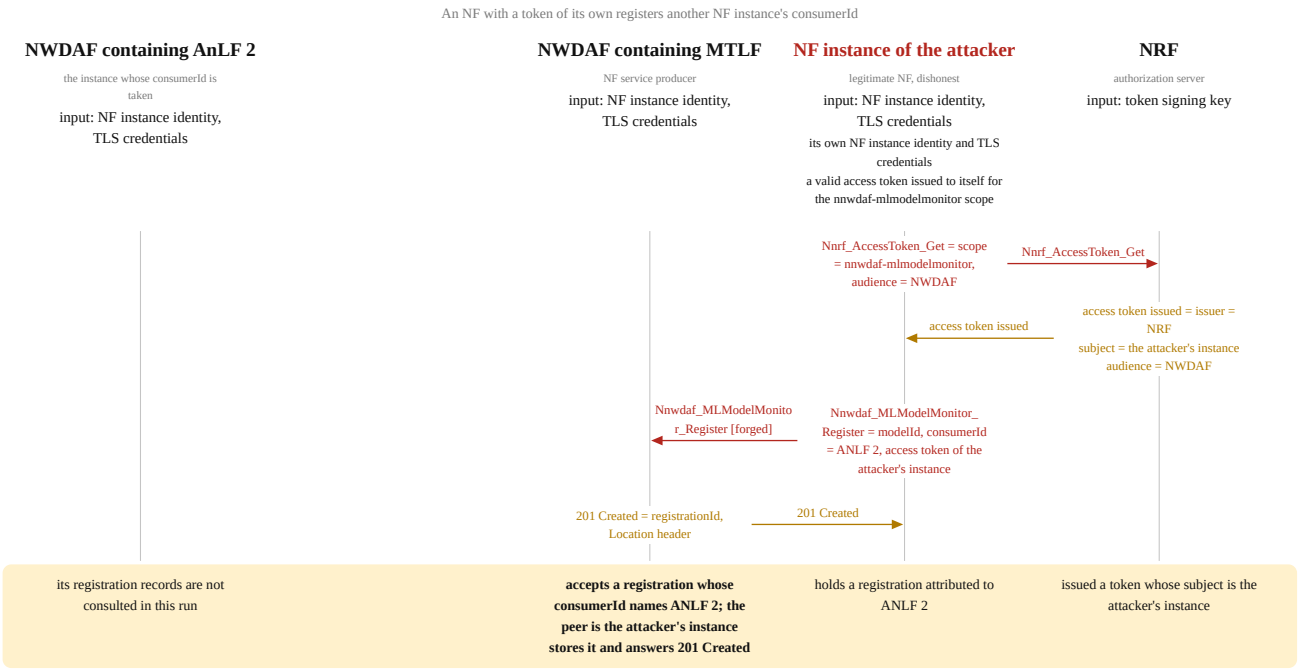
发生了什么。 A NWDAF号案件,持有其自己的有效出入证,其中援引Nnwdaf_MLModelMonitor_Register和AnLF号案件的consumerId。 包含MTLF的NWDAF号机对象征性签名,其发行人,受众,范围及主体进行对照TLS客户端证书的验证,然后存储注册和答案201 以registrationId号机创建. 存储的注册名称是另一个例子作为消费者。

攻击者需要什么。 自己的NF00个实例身份及其TLS的证书,以及NRF为nwdaf-mlmodelmonitor范围签发的1个访问令牌。 没有损坏的密钥,也不需要其他证书,该实例使用它自己与生产者的TLS会话。

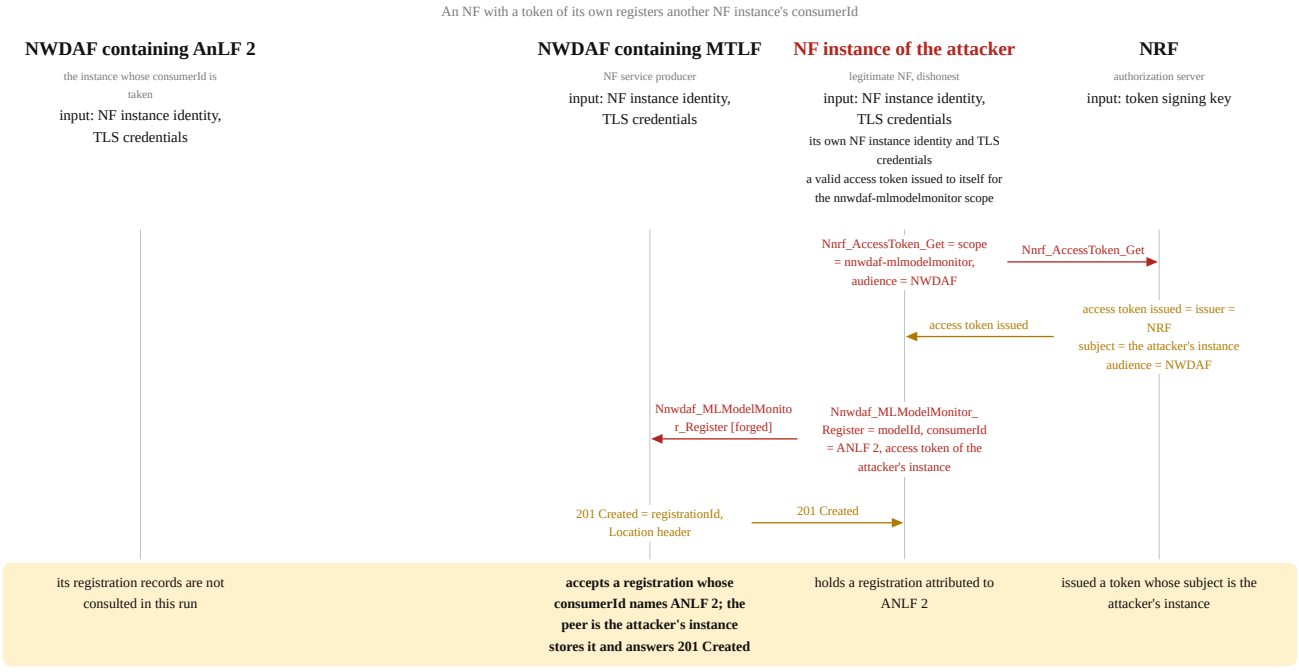
攻击者能得到什么。 生产者的登记记录,以及从这些记录中得出的关于ML型号使用何种实例的所有信息,可以用来命名一个从未问过的实例。 一个阅读记录的操作员将监控归属于错误的NF.



- 图2。 NF号有自己登记标志的 NF号案是consumerId号案 财产A07; 攻击查询 a07_body_nf. *



- 图3。 NF号有自己登记标志的 NF号案是consumerId号案 财产Z03; 攻击查询 a07_body_nf. *



- 图4。 NF号有自己登记标志的 NF号案是consumerId号案 财产U03; 攻击查询 a07_body_nf. *

拟议修改。 在登记册处理中,比较consumerId(或 减)consumerSetId会 议 纪 要MLModelMonitorReg身体与身体NF实例ID标记对象和经认证的TLS委托人,当他们有分歧时,拒绝他们的请求。 在模型的复制上检查了这个变化:攻击查询被验证,正常运行仍然被找到,没有其他记录的答案变化.

用 ProVerif复核。 改动已纳入模型副本:Nnwdaf_MLModelMonitor_Register处理,在签章检查后,NWDAF包含MTLF比较consumerId(分别为:consumerSetId会 议 纪 要MLModelMonitorReg身体与身体NF实例ID标记对象和经认证的TLS客户端,并在请求有分歧时拒绝。 在改变的模型上ProVerif证明`a07_body_nf`: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43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/0049-fix-consumerid.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
A02	**NF项请求的认证实例。** 每当含 MTLF 的 NWDAF 接受一次注册/订阅/通知/反馈请求时，存在一个真实运行的、以该 MTLF 实例为对端的含 AnLF 的 NWDAF 运行（反之亦然），身份粒度固定为 NF 实例。	无	成立	中	是
A03	**通知值与订阅值相符。** 每次含 MTLF 的 NWDAF 接受通知时，存在匹配的含 AnLF 的 NWDAF 运行，且 modelId(s)、notifCorrId、notificationUri、mLEvent/mLEventFilter/tgtUe 与订阅时各方本地值一致；每次含 AnLF 的 NWDAF 接受订阅时，存在匹配的含 MTLF 的 NWDAF 运行，且 modelIds 与 notifCorrId 一致。	无	成立	中	是
A04	**每项创建的专项资源。** 每次含 MTLF 的 NWDAF 接受一次注册创建，对应不同的含 AnLF 的 NWDAF 运行（registrationId 单射）；每次含 AnLF 的 NWDAF 接受一次订阅创建，对应不同的含 MTLF 的 NWDAF 运行（subscriptionId 单射）。	无	成立	低	否
A07	**consumerId与经认证的消费者匹配。** 每次含 MTLF的 NWDAF接受注册/订阅时，请求体中的 consumerId与令牌 主题,TLS客户端证书中的 NF 实例 ID一致，且令牌 发行者为允许的 NRF- 观众匹配本实例。	无	不成立（1 个攻击）	中	不确定
A08	**通知属于先前的订阅。** 每次含 MTLF的 NWDAF 接受通知时，notifCorrId与 notificationUri对应一个此前由该消费者建立的订阅，modelAccuInfos/anaFeedbacks中的 modelId属于该订阅的 modelIds，且请求所用令牌 范围覆盖该操作。	无	成立	中	是
K01	**长期密钥保密。** 外部攻击者与持有自身凭据的恶意 NF 均不能推导出 NRF 的令牌签名私钥、NRF 与生产者之间的共享对称密钥，或其他 NF 的 TLS 会话密钥。	无	成立	低	是
K02	**准确性和反馈保密性。** 通知中的 modelAccuInfos、anaFeedbacks 以及订阅/注册中的 tgtUe 只对建立该订阅的含 MTLF 的 NWDAF 与含 AnLF 的 NWDAF 可见；其他合法 NF 与外部攻击者不能获得。	无	攻击成立（文稿已写明）	中	是
D01	**通知真实性和完整性。** 每次含 MTLF 的 NWDAF 接受通知时，存在含 AnLF 的 NWDAF 的真实发送，且 notifCorrId、modelAccuInfos/anaFeedbacks 与发送时一致。	无	攻击成立（文稿已写明）	中	是
Z01	**每一份请求都带有有效的符号。** 每次含 MTLF或含 AnLF的 NWDAF提交注册、订阅、退订、更新或通知操作时，存在由允许的 NRF签发的、未过期、观众匹配本实例、范围覆盖该操作的令牌，且令牌 主题与请求者身份一致。	无	成立	低	是

ID	性质	假定的泄露	结果	价值	文稿是否已写
Z03	**受呼叫者约束的主体。** 每次令牌被用于服务请求时，令牌 主题与请求者 TLS证书身份一致，观众匹配被请求的生产者实例，范围覆盖被请求的操作，且请求体中的 consumerId与 主题一致。	无	不成立（1 个攻击）	中	不确定
Z05	**无法获得其他NF资源。** 在允许控制一个合法 NF 域（含其自身凭据与令牌）的前提下，该域不能读取或修改其他 NF 的注册、订阅，也不能向其他 NF 的 notificationUri 投递通知；被攻陷的 TLS 终结代理不能读取其他端点的 TLS 会话。	无	成立	中	是
U01	**Feedback 绑定在模型和订阅上。** 每次含 MTLF 的 NWDAF 接受含 anaFeedbacks 的通知时，反馈中的 modelIds、发送方身份与 notifCorrId 均与一个此前建立的订阅一致。	无	成立	中	是
U02	**外部 vs 损坏的中介。** 在外部攻击者配置与被攻陷中间实体配置下分别检查通知完整性与订阅授权绑定，并比较两者结论。	TLS 终结代理或 SCP (在订阅建立之后、通知投递之前)	攻击成立（文稿已写明）	中	是
U03	**各种资源中的恶意NF。** 在恶意合法 NF 持有自身有效令牌的前提下，检查其能否操作其他 NF 的注册、订阅或通知，并归因于规范文本或本地策略。	无	不成立（1 个攻击）	中	不确定
X01	**通知重新播放保护。** 载有MTLF的NWDAF型飞机两次接受的每份通知,均由载有AnLF的NWDAF型飞机两次发出:POST型飞机的重播通知是第二次不接受的。	无	攻击成立（文稿已写明）	低	是

“攻击成立（文稿已写明）”：证明器找到了这个攻击，而文稿自己已经写明它存在。这条性质不成立；这是已知结果，不算发现（附录 B）。

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: 反馈与模型、报告者、监控订阅绑定	就通知字段而言,反馈与订阅的模型标识符和该订阅的生产者实例有关:反馈要素除了以同样的notifCorrId进行旅行之外,没有单独的约束,其事件阵列也不是模拟的。	U01, A08, D01
Q2: 外部篡改与被攻陷中间实体结果明确区分	这两种配置与来源完全不同:从网络上看,通知不能被读取、更改或重播,而一个受损的TLS终止代理可以读取,替换有效载荷并两次发送通知,因为通知操作没有符号。	U02, K02, D01, X01
Q3: 恶意合法 NF 的跨资源操作是否构成规范缺口或仅本地策略条件	规格中的一个空白是缺少consumerId美元与经认证的消费者的比较,这使一个实例登记在另一个实例的身份之下; 其余是地方政策,因为API界定了单一服务级别范围,而恶意NF的图案资源识别特征仍不为人所知。	U03, A07, Z05, Z03

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是一个经过认证的每页密钥下的保密通道; 握手、证书链和密钥确认没有建模。
- 重放请求不能代表:模型的请求表非ces超近似,所以A04只在其标识读数中解答.

- 访问令牌是用有效标记而不是时间在债权上签名; 期满和不撤销的,不予行使。
- 观众模式仅为NF型; 实例一级的受众以及切片和NF Set的主张要求不是模拟的。
- consumerSetId,mLEvent,mLEventFilter和tgtUe没有建模,notificationUri号机车作为订户自己的终点处理.
- 通知有效载荷是一个不透明的值; 如任务所述,准确性的数字正确性不在模型之外。
- 一方储存的密钥和NRF型密钥的折合不作模型; 2. 攻击者是网络 恶意的NF 拥有自己的证书 和TLS 终止代理 AnLF -MTLF的链接。
- 只有API子流:NRF的授权决定,发现,SCP转发规则和没有相互TLS的间接通信不在模型之外.
- 不问原始人的可用性、时间和计算强度。

主持人记录的是什么:

- 没带对照查询的证明（附录 C）： A03: a03_bind, A04: a04_reg_id, A04: a04_sub_id, A07: a07_tls, A08: a08_bind_net, A08: a08_bind_nf, Z01: z01_reg, Z01: z01_sub, Z03: a07_tls, Z05: a08_bind_nf, U01: a08_bind_net, U01: a08_bind_nf, U03: d01_nf, U03: z05_regid。 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:NF 对请求的认证

每当含 MTLF 的 NWDAF 接受一次注册/订阅/通知/反馈请求时，存在一个真实运行的、以该 MTLF 实例为对端的含 AnLF 的 NWDAF 运行（反之亦然），身份粒度固定为 NF 实例。

仅针对网络,消费者或生产者所接受的每一份登记、订阅和通知,就相当于根据该请求认证的NF个实例,因此,单凭网络攻击者无法产生接受。 财产为NF个零颗粒,因此,持有自己证书的一方被视为一个真实的例子,这就是服务的目的。

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:服务的核心认证担保,在任何几个会话中都得到证明:不是新的,而是其余审查所依赖的财产.
- 在文件中说明:是的。 文件上写着:s0472、s0480、s0412
- 休息时间:TLS系仿照对一对例的密钥,作为经认证的保密通道; 握手方式不是模拟的; 该标志是NRF号的签字,以代替其主张; 查询中的断开通过排除恶意NF或代理行为痕迹来表达网络唯一攻击者

A03: 通知值与订阅值相符

每次含 MTLF 的 NWDAF 接受通知时，存在匹配的含 AnLF 的 NWDAF 运行，且 modelId(s)、notifCorrId、notificationUri、mLEvent/mLEventFilter/tgtUe 与订阅时各方本地值一致；每次含 AnLF 的 NWDAF 接受订阅时，存在匹配的含 MTLF 的 NWDAF 运行，且 modelIds 与 notifCorrId 一致。

消费者接受的通知携带了消费者创建的notifCorrId和订阅的模型标识符,因此网络上没有人可以给错误的订阅附加通知. 关于mLEvent,mLEventFilter和tgtUe的协议在来源中只是应该的,没有模仿,所以对此一言不发.

- 结果:持有; 回答问题:是的; 可用备注
- 数值介质:将通知附在订阅时是约束; 排除可选属性是一个真正的限制。
- 在文件中说明:是的。 文件上说:s0076、s0122、s0126、s0319
- 休息时间:mLEvent,mLEventFilter财务报告和财务报告tgtUe- 没有建模; (b) 来文提交人说,他们同意应(s0319);modelIds是一个值,而不是数组; 因此不存在失败的变体

A04: 每项创造的不同资源

每次含 MTLF 的 NWDAF 接受一次注册创建，对应不同的含 AnLF 的 NWDAF 运行（registrationId 单射）；每次含 AnLF 的 NWDAF 接受一次订阅创建，对应不同的含 MTLF 的 NWDAF 运行（subscriptionId 单射）。

生产者和消费者指派的识别标志是注射式的:两个装有相同registrationId或subscriptionId的验收是相同的验收. 更强的读法,一个请求从未两次被接受,在模型中因重播请求而失败,TLS记录层在协议中阻止,模型无法表达,因此失败不作为协议的弱点提出.

- 结果:持有; 回答问题:部分; 可用备注
- 价值低:经证明的部分来自资源创造语义; 有趣的部分取决于 重播保护 模型不能代表。
- 在文件中说明:否。 资料来源:s0049、s0050、s0051、s0085、s0087。

- 休息: 重播保护由请求表模拟,该表为:ProVerif超近似值,所以模型中接受重复请求; 2. 被证明的部分是关于标识符的,而不是关于请求

A07:consumerId与经认证的消费者相符

每次含 MTLF的 NWDAF接受注册/订阅时，请求体中的 consumerId与令牌 主题,TLS客户端证书中的 NF实例 ID一致，且令牌 发行者为允许的 NRF- 观众匹配本实例。

信使标的总是来电者TLS客户端证书上的身份,因此一个被盗信使不能被另一个实例使用. 请求机构的consumerId与该身份无关:在另一个机构consumerId下,一个拥有自己登记簿有效标志的事例,由生产者储存。

- 结果:失败(1次攻击); 回答问题:是的; 可用
- 值介质:恶意法律NF在不突破任何密码步骤的情况下获得对另一个实例的假归属监测,去除它的更改很小,并被检查.
- 在文件中说明:不明确。 资料来源:s0040、s0041、s0042、s0480。
- 休息:来源不需要比较,所以攻击是根据书面的规格; 受众模式仅为NF型; 过期为有效标记; 模型中不存在过期的符号

A08:通知属于较早的订阅者

每次含 MTLF的 NWDAF接受通知时，notifCorrId与 notificationUri对应一个此前由该消费者建立的订阅，modelAccuInfos/anaFeedbacks中的 modelId属于该订阅的 modelIds，且请求所用令牌 范围覆盖该操作。

接受的通知与早先创建的消费者的订阅有关:其notifCorrId和型号识别标志是该订阅的、针对网络的、针对恶意的NF和针对受损的代理的。 通知行动没有进入标志,因此没有要求范围; 剩下的是有效载荷的完整性, 单独询问。

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:它显示哪些部分的通知绑定在一个受损害的中间体存活下来,哪些没有。
- 在文件中说明:是的。 文件上说:s0076、s0122、s0126、s0347、s0412
- 休息时间:notificationUri型机车仿照用户自己的端点; 重新定向不是模拟的; 有效载荷内容不受此属性的约束,只有识别器

K01:长期密钥保密

外部攻击者与持有自身凭据的恶意 NF 均不能推导出 NRF 的令牌签名私钥、NRF 与生产者之间的共享对称密钥，或其他 NF 的 TLS 会话密钥。

NRF签名密钥,NRF与一个生产者共享的密钥,以及端点对的TLS密钥,都不是网络攻击者或拥有自己资质的恶意NF所衍生出来的. 在一个链接上损坏的代理不会暴露其不终止的链接的会话 。

- 结果:持有; 回答问题:是的; 可用
- 数值低:它来自不可理解的建模密钥; 其价值是孤立部分。
- 在文件中说明:是的。 文件上写着:s0405、s0439、s0475
- 休息:将密钥理想化为可忽略的私人值; 正在读取 party 的密钥存储器不是模拟的

K02:准确性和反馈保密性

通知中的 modelAccuInfos、anaFeedbacks 以及订阅/注册中的 tgtUe 只对建立该订阅的含 MTLF 的 NWDAF 与含 AnLF 的 NWDAF 可见；其他合法 NF 与外部攻击者不能获得。

准确性信息和分析反馈仅见于两起针对网络和恶意NF的订阅NWDAF例. 终止该链接的TLS攻击者读了这些内容,消息来源说,必须接受这些内容,因为各方必须信任SCP。

- 结果:攻击停留(在文件中说明); 回答问题:是的; 可用
- 值介质:它绘制出监测数据来源的保密界限。
- 在文件中说明:是的。 文件上写着:s0125、s0126、s0472
- 剩余:一个有效载荷值为modelAccuInfos和anaFeedbacks; tgtUe号没有在模型的信息中携带

D01:通知的真实性和完整性

每次含 MTLF 的 NWDAF 接受通知时，存在含 AnLF 的 NWDAF 的真实发送，且 notifCorrId、modelAccuInfos/anaFeedbacks 与发送时一致。

针对网络和恶意的NF, 消费者接受的通知是由该订阅的制作人发出的,其中附有该相关标识符和有效载荷,notifCorrId号保留了重复播放的通知两次不被接受。 针对终止双人TLS号的攻击者,消费者接受制作人从未发出的通知,因为通知没有标志,也没有自己的签名.

- 结果:攻击停留(在文件中说明); 回答问题:是的; 可用
- 数值介质:预期是正面的; 负面给出了可以伪造监测数据的确切条件。
- 在文件中说明:是的。 文件中说:ts-33-501:2921,s0122,s0123,s0126,s0412
- 中止:终止TLS的代理通过给攻击者提供这种联系的双向模式; 来文方称,通知中没有符号。

Z01: 每一份请求都带有有效的代号

每次含 MTLF或含 AnLF的 NWDAF提交注册、订阅、退订、更新或通知操作时，存在由允许的 NRF签发的、未过期、观众匹配本实例、范围覆盖该操作的令牌，且令牌 主题与请求者身份一致。

每次接受的注册和订阅都带有向提交该注册的事例发放的NRF的代号,受众为NWDAF和单一服务范围,以及生产者检查签发人、签名、对象和受众。 过期检查在模型中存在,但无法在其中构建过期的令牌,来源表示不支持撤销.

- 结果:持有; 回答问题:部分; 可用备注
- 低值:按规定进行符号检查; 模型不能锻炼的两部分是有趣的、过期的和范围颗粒性的。
- 在文件中说明:是的。 文件上写着:s0344,s0345,s0450,s0474,s0485,s0487,s0412
- 休息时间:观众为NF人,来源允许; 过期为有效标记,不行使; 一个服务级别范围意味着范围检查从未区分操作

Z03: 与呼叫者绑定的托肯主体

每次令牌被用于服务请求时，令牌 主体 与请求者 TLS 证书身份一致， 观众 匹配被请求的生产者实例， 瞄准镜 覆盖被请求的操作，且请求体中的 consumerId 与 主体 一致。

制作方可以放心,代币是发给呈递方的:主体与TLS客户证相符,观众为自己的NF型,范围覆盖服务范围. consumerId的机构不受该约束,因此,登记记录可以由打电话者选择,如A07。

- 结果:失败(1次攻击); 回答问题:是的; 可用
- 值介质:正值部分确认约束源要求的主体; 2. 消极的一面是审查的实质性差距。
- 在文件中说明:不明确。 资料来源:s0474、s0480、s0482、s0485、s0487。
- 休息时间:观众为NF型,来源允许; consumerSetId的替代品没有模型化

Z05:无法使用其他NF资源.

在允许控制一个合法 NF 域（含其自身凭据与令牌）的前提下，该域不能读取或修改其他 NF 的注册、订阅，也不能向其他 NF 的 notificationUri 投递通知；被攻陷的 TLS 终结代理不能读取其他端点的 TLS 会话。

恶意的NF无法再获得NF的注册或订阅标识符,也无法学习另一个NF的订阅的关联标识符,因此通知只送达了创建订阅的消费者; 2. 这些识别资料是两码事之间的唯一问题。 在一个链接上失密的代理不会暴露其他链接. 无法保证的是资源一级的授权:每个允许的例子都可以援引每一项业务,但有一个服务一级的范围。

- 结果:持有; 回答问题:是的; 可用备注
- 价值介质:它表明单一服务级别范围不能通过模型中的可猜测的手柄加以利用,并标出需要资源级别范围的标志.
- 在文件中说明:是的。 文件上写着:s0347、s0397、s0485
- 休息:资源层面的授权不是模拟的; 保护另外NF的资源取决于其识别特征是否不可理解; notificationUri 是用户自己的终点

U01: 用于模型和订阅的反馈

每次含 MTLF 的 NWDAF 接受含 anaFeedbacks 的通知时，反馈中的 modelIds、发送方身份与 notifCorrId 均与一个此前建立的订阅一致。

接受的通知中的分析反馈是指消费者订阅的模型识别符,来自该订阅的制作人,针对网络和恶意的NF. 反馈中的事件阵列没有建模,因此它与分析识别符的绑定性没有被涵盖.

- 结果:持有; 回答问题:是的; 可用备注
- 值介质:它回答了用户的问题:反馈不能附加到另一个模型上,也不能从另一个实例中到达.
- 在文件中说明:是的。 文件上说:s0122、s0126、s0076、s0328
- 停留:一个有效载荷值为anaFeedbacks; 其事件元素没有建模

U02: 外部对被破坏的中间人

在外部攻击者配置与被攻陷中间实体配置下分别检查通知完整性与订阅授权绑定，并比较两者结论。

两种配置不同. 单凭网络,通知不能被读取、更改或伪造。 如果一个损坏的TLS终止代理,有效载荷可以读取,一个从未发送的生产者通知可以交付,一个录制的可以再次交付. 不同之处恰恰是SCP中来源的信任.

- 结果:攻击停留(在文件中说明); 回答问题:是的; 可用
- 值介质:它用确切的边界来回答问题,并复制源描述的一个结果,所以它是确认已知的结果而不是新的弱点.
- 在文件中说明:是的。 这些文件都说:ts-33-501:2921,ts-33-501:2873,s0412,s0122,s0126
- 休息:代理持有终止链接的双向,这就是终止TLS的含义; 在订阅后和通知前,代理机会失密

U03:各种资源中的恶意NF

在恶意合法 NF 持有自身有效令牌的前提下，检查其能否操作其他 NF 的注册、订阅或通知，并归因于规范文本或本地策略。

部分答案是案文中的空白,部分答案是地方政策。 空隙:任何带有有效令牌的实例都可以在另一个实例的consumerId下注册,因为身体属性从未与认证身份相比过. 政策:一个服务级别范围,可以援引NRF授权和当地配置决定的操作,其他实例的资源识别特征为恶意NF所未知,因此无法在模型中操作.

- 结果:失败(1次攻击); 回答问题:是的; 可用
- 值介质:它将编辑器在文本中必须修正的内容与操作员必须配置的内容区分开来.

- 在文件中说明:不明确。 资料来源:s0347、s0394、s0397、s0485。
- 休息:资源一级的授权留给地方政策,而不是模拟; 标识符是新的可忽略的值

X01:通知重播保护

双方接受的每份通知NWDAF包含MTLF曾两次送来NWDAF包含AnLF: 重播的通知POST不再接受第二次申请。

针对网络,两次收到接受的通知:关联标识符和模型标识符将每次接受与订阅绑定,重播记录不通过. 对于终止TLS对对子的攻击者,可以给生产者发送的一方发出第二次通知,因为通知中没有任何内容区分代理方再次交付.

- 结果:攻击停留(在文件中说明); 回答问题:是的; 可用
- 值低:是D01的结果:相同的保护与同样的失败,所以增加了重播读数而不是新的结果.
- 在文件中说明:是的。 文件上说:ts-33-501:2921,s0122,s0123,s0412
- 休息:TLS的回放保护是用一个请求非目录表模拟的,因此通过notifCorrId装订要求财产; 通知没有符号

附录 B：复现的已知结论

某一财产如文件已经说明的那样失效,或被搁置,并不是一个结论。 如下是此类: 分析在模型上复制,给出了确切的条件.

B.1 A损坏 SCP 重写它携带的准确性通知

类型	协议规范本身的弱点
文稿出处	ts-33-501:2921, ts-33-501:2873
价值	中
涉及的性质	D01, K02, U02, X01 （见第 3 节）
依据	ProVerif 攻击询问 `d01_ctl`,`k02_ctl`,`x01_ctl`

发生了什么。 A TLS终止在两个NWDAF例之间联系的代理阅读了准确性和反馈有效载荷,并重新加密给消费者一份通知,其订阅内容为notifCorrId和modelId,但生产者从未发送过有效载荷。 消费者接受它并回答204 No Content,因为通知操作没有带访问符,其唯一的保护是代理终止的TLS会话. 记录的通知也可以第二次送达。

攻击者需要什么。 对《公约》SCP或 时 间TLS终止该链接上的代理,这意味着该链接的双向TLS在订阅之后和发出通知之前,会议即告结束。 网络攻击者独自一人无法做到这一点。

攻击者能得到什么。 消费者对一个模型表现如何的看法及其作用的反馈,都在代理人的控制之下,一份通知可以发出两次。

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_reg	检查		证明:3
A03	proved		a03_bind			证明:1
A04	proved		a04_reg_id		a04_reg (model_artifact); a04_sub (model_artifact)	证实2,2次攻击
A07	proved		a07_tls	3中的1人	a07_body_nf (holds_in_source)	证实3,1次攻击
A08	proved		a08_bind_net			证明:3
K01	proved		k01_nrfkey	检查		证明:5
K02	proved		k02_net	检查	k02_ctl (holds_in_source)	证实2,1次攻击
D01	proved		d01_net	检查	d01_ctl (holds_in_source)	证实2,1次攻击
Z01	proved		z01_reg			证明:2
Z03	proved		a07_tls	3中的1人	a07_body_nf (holds_in_source)	证实3,1次攻击
Z05	proved		z05_regid	5中的4人		证明:5
U01	proved		a08_bind_net	4中的2人		证明:4
U02	proved		d01_net	检查	d01_ctl (holds_in_source); k02_ctl (holds_in_source)	证实2,2次攻击
U03	proved		d01_nf	5中的3人	a07_body_nf (holds_in_source)	证实5,1次攻击
X01	proved		x01_net	检查	x01_ctl (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	联合国对登记的每一次接受NWDAF包含MTLF对应于真实运行NF(a) 请求中认证的事例; 攻击者只有网络	network	proved	a02_reg	检查
A02	联合国对订阅的每次接受NWDAF包含AnLF对应于真实运行NF(a) 请求中认证的事例; 攻击者只有网络	network	proved	a02_sub	检查
A02	联合国对通知的每份接受NWDAF包含MTLF对应于真实运行NWDAF包含AnLF被证实的; 攻击者只有网络	network	proved	a02_not	检查
A03	接受通知的notifCorrId和modelIds是该消费者先前创建的认购通知; 攻击者只有网络	network	proved	a03_bind	无
A04	每个被接受的登记设定都对应一个不同的登记请求运行,因此没有两项接受来自一项请求; 攻击者只有网络	network	攻击 (model_artifact)	a04_reg	
A04	每个被接受的订阅创建都对应一个不同的订阅请求运行,因此没有一个接受来自一个请求; 攻击者只有网络	network	攻击 (model_artifact)	a04_sub	
A04	registrationId型是注射式的:两种装有相同registrationId型的接受式是相同的接受式,因此没有两种登记请求得到相同的识别码; 2. 攻击者只有网络	network	proved	a04_reg_id	无

目标	主张	攻击者	回答	查询	对照
A04	subscriptionId型是注射式的:两个装有相同subscriptionId型的接受式是相同的接受式,因此没有两个订阅请求得到相同的识别码; 攻击者只有网络	`network`	proved	a04_sub_id	无
A07	信使对象为来电者的TLS客户证书身份; 2. 攻击者只有网络	`network`	proved	a07_tls	无
A07	信使对象为来电者的TLS客户证书身份; 2. 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	a07_tls	无
A07	请求体中的consumerId是经认证的代币消费者; 2. 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	攻击 (holds_in_source)	a07_body_nf(控制 a07_body_net) (中文(简体)).	
A07	请求体中的consumerId是经认证的代币消费者; 2. 攻击者只有网络	`network`	proved	a07_body_net	检查
A08	接受通知的notifCorrId和modelIds属于先前创建的MTLF的订阅,没有提出象征性范围,因为OAuth2不适用于通知业务; 攻击者只有网络	`network`	proved	a08_bind_net	无
A08	接受通知的notifCorrId和modelIds属于先前创建的MTLF的订阅,没有提出象征性范围,因为OAuth2不适用于通知业务; 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	a08_bind_nf	无
A08	接受通知的notifCorrId和modelIds属于先前创建的MTLF的订阅,没有提出象征性范围,因为OAuth2不适用于通知业务; 攻击者持有 TLS 连接的双向 它终止在那对。	`scp_compromised`	proved	a08_bind_nf	无
K01	NRF符号签名密钥是无法运算的; 攻击者只有网络	`network`	proved	k01_nrfkey	检查
K01	NRF符号签名密钥是无法运算的; 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	k01_nrfkey	检查
K01	端点对的TLS会话密钥不能由第三方产生; 2. 攻击者只有网络	`network`	proved	k01_tlskey	检查
K01	端点对的TLS会话密钥不能由第三方产生; 2. 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	k01_tlskey2	检查
K01	NRF型机车与制片人共享的密钥不能衍生; 2. 攻击者只有网络	`network`	proved	k01_tlskey2	检查
K02	精度和反馈有效载荷没有被终止对称的TLS的攻击者所了解.	`scp_compromised`	攻击 (holds_in_source)	k02_ctl(控制k02_net) (中文(简体)).	
K02	网络攻击者没有掌握通知的准确性和反馈有效载荷。	`network`	proved	k02_net	检查
K02	一份通知的准确性和反馈有效载荷没有通过持有自己证书的恶意NF人得知。	`malicious_nf`	proved	k02_nf	检查
D01	NWDAF型飞机发出一份接受的通知,载有AnLF的订货,其中notifCorrId和该有效载荷; 攻击者只有网络	`network`	proved	d01_net	检查
D01	已接受的通知系由缔约方大会发出。NWDAF包含AnLF签署书,其中:notifCorrId和该有效载荷,甚至对攻击者终止TLS一对夫妇。	`scp_compromised`	攻击 (holds_in_source)	d01_ctl(控制d01_net) (中文(简体)).	
D01	NWDAF型飞机发出一份接受的通知,载有AnLF的订货,其中notifCorrId和该有效载荷; 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	d01_nf	检查
Z01	每一经接受的登记都附有由联合王国政府签发的证书。NRF页:1NF(a) 向该生产者的受众介绍单一服务范围和有效(未到期)有效性的实例; 攻击者只有网络	`network`	proved	z01_reg	无

目标	主张	攻击者	回答	查询	对照
Z01	每一个被接受的订阅都带有NRF向NF案出具的代币,该代币的受众为这名制作人、单一服务范围和有效(未到期)有效; 攻击者只有网络	`network`	proved	z01_sub	无
Z03	标志性主体是其TLS客户端证书上的来电者的身份; 2. 攻击者只有网络	`network`	proved	a07_tls	无
Z03	标志性主体是其TLS客户端证书上的来电者的身份; 2. 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	a07_tls	无
Z03	请求机构内的consumerId是批准请求的标志; 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	攻击 (holds_in_source)	a07_body_nf(控制 a07_body_net) (中文(简体)).	
Z03	请求机构内的consumerId是批准请求的标志; 攻击者只有网络	`network`	proved	a07_body_net	检查
Z05	通知只送达开户消费者的终点,而不再送达NF's notificationUri; 3. 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	a08_bind_nf	无
Z05	恶意的NF人无法再学习NF的registrationId,因此无法操作该注册; 攻击者只有网络	`network`	proved	z05_regid	检查
Z05	恶意的NF人无法再学习NF的registrationId,因此无法操作该注册; 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	z05_regid	检查
Z05	恶意的NF无法得知另外NF的订户的notifCorrId,因此不能向它发出通知; 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	z05_corr	检查
Z05	在AnLF-MTLF链接上失密的代理并不暴露其他端点的TLS会话,这里是NRF的链接; 攻击者持有 TLS 连接的双向 它终止在那对。	`scp_compromised`	proved	k01_tlskey	检查
U01	接受的通知中的modelIds份分析反馈属于该消费者的订阅; 攻击者只有网络	`network`	proved	a08_bind_net	无
U01	接受的通知中的modelIds份分析反馈属于该消费者的订阅; 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	a08_bind_nf	无
U01	接受的通知中的反馈来自订户的NWDAF,其中AnLF来自其他寄信人; 攻击者只有网络	`network`	proved	d01_net	检查
U01	接受的通知中的反馈来自订户的NWDAF,其中AnLF来自其他寄信人; 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	d01_nf	检查
U02	针对终止TLS对对子的通知内容的攻击者,可以修改:消费者接受生产者从未发送的通知.	`scp_compromised`	攻击 (holds_in_source)	d01_ctl(控制d01_net) (中文(简体)).	
U02	针对终止TLS对对子的攻击者,可以读取通知的有效载荷.	`scp_compromised`	攻击 (holds_in_source)	k02_ctl(控制k02_net) (中文(简体)).	
U02	对外部网络攻击者而言,通知内容不能修改或伪造:生产者随该有效载荷发出了接受的通知。	`network`	proved	d01_net	检查
U02	对照外部网络攻击者,无法读取通知的有效载荷。	`network`	proved	k02_net	检查
U03	恶意的NF不能阅读或伪造另外NF订阅的通知; 2. 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	d01_nf	无
U03	恶意NF无法再获得NF的注册或订阅手柄; 2. 攻击者拥有自己的NF证书和有效标志。	`malicious_nf`	proved	z05_regid	无

目标	主张	攻击者	回答	查询	对照
U03	持有自己有效代币的恶意NF可以再操作NF的资源:它可以用NF的consumerId进行注册.	malicious_nf	攻击 (holds_in_source)	a07_body_nf(控制 a07_body_net) (中文(简体)).	
U03	仅凭网络本身,就不接受其consumerId不是经认证的消费者的请求,因此网络攻击者不能让NF再操作NF的资源.	network	proved	a07_body_net	检查
U03	仅凭网络,无法伪造或读取NF的订阅通知。	network	proved	d01_net	检查
U03	仅凭这个网络就无法获得另外NF的注册手柄,因此另外NF的注册无法运行.	network	proved	z05_regid	检查
X01	消费者两次接受的通知被制作人两次发出,甚至针对终止了TLS对对子的攻击者.	scp_compromised	攻击 (holds_in_source)	x01_ctl(控制x01_net) (中文(简体)).	
X01	生产者两次发出消费者接受的两次通知:notifCorrId号装订书拒绝重复播放的通知; 攻击者只有网络	network	proved	x01_net	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-20261115T083926, 2026-11-15. 状态: 完成 。 型号:deepseek-v4-1-flash-261017. 台阶:62,校对:28 s,壁19 min,耗资0.179 USD.

背景:主机从谈话中移除了1时间(s),总共删除了465071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:229 证明运行,228 决定,1 未答,21 s,75 答录.

分析了什么

协议	审查ML型号监测与SBA隔离
版本	19.8.0
分析范围	复核首轮 Nnwdaf_MLModelMonitor:登记/登记/通知/准确的反馈;严格按端点隔离 TLS，身份与符号主题绑定；外部攻击者、恶意消费者、被攻陷 TLS终结代理必须分成明确独立配置。精度是 不透明数据，不证明数值正确性。
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661个编号段落(251766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	4.7	Nnwdaf_MLModelMonitor 服务
主体	4.7.1	服务说明
主体	4.7.1.1	概览
主体	4.7.1.2	服务架构
主体	4.7.1.3	网络函数
主体	4.7.1.3.1	网络数据分析函数(NWDAF)
主体	4.7.1.3.2	NF 服务消费者
主体	4.7.2	服务业务
主体	4.7.2.1	导言
主体	4.7.2.2	Nnwdaf_MLModelMonitor_Register次服务业务
主体	4.7.2.2.1	A. 概况
主体	4.7.2.2.2	登记对ML模型分析精度的监测
主体	4.7.2.3	Nnwdaf_MLModelMonitor_Deregister次服务业务
主体	4.7.2.3.1	A. 概况

文稿	章节	标题
主体	4.7.2.3.2	调整对ML型号分析精度的监测
主体	4.7.2.4	Nnwdaf_MLModelMonitor_Subscribe次服务业务
主体	4.7.2.4.1	A. 概况
主体	4.7.2.4.2	订阅监测通知
主体	4.7.2.4.3	更新对监测通知的订阅
主体	4.7.2.5	Nnwdaf_MLModelMonitor_Unsubscribe次服务业务
主体	4.7.2.5.1	A. 概况
主体	4.7.2.5.2	未订阅监测通知
主体	4.7.2.6	Nnwdaf_MLModelMonitor_Notify次服务业务
主体	4.7.2.6.1	A. 概况
主体	4.7.2.6.2	关于订阅活动的通知
主体	5.6	Nnwdaf_MLModelMonitor服务 API
主体	5.6.1	导言
主体	5.6.2	使用费HTTP美元
主体	5.6.2.1	A. 概况
主体	5.6.2.2	HTTP标准标题
主体	5.6.2.2.1	A. 概况
主体	5.6.2.2.2	内容类型
主体	5.6.2.3	HTTP 个自定义标题
主体	5.6.3	资源
主体	5.6.3.1	资源结构
主体	5.6.3.2	资源:NWDAF ML 模式监测登记
主体	5.6.3.2.1	说明
主体	5.6.3.2.2	资源定义
主体	5.6.3.2.3	资源标准方法
主体	5.6.3.2.3.1	POST
主体	5.6.3.2.4	资源自定义操作
主体	5.6.3.3	资源:个人 NWDAF ML 模型监测登记
主体	5.6.3.3.1	说明
主体	5.6.3.3.2	资源定义
主体	5.6.3.3.3	资源标准方法
主体	5.6.3.3.3.1	DELETE
主体	5.6.3.3.4	资源自定义操作
主体	5.6.3.4	资源:NWDAF ML 模式监测订阅
主体	5.6.3.4.1	说明
主体	5.6.3.4.2	资源定义

文稿	章节	标题
主体	5.6.3.4.3	资源标准方法
主体	5.6.3.4.3.1	POST
主体	5.6.3.4.4	资源自定义操作
主体	5.6.3.5	资源:个人 NWDAF ML 型号监测订阅
主体	5.6.3.5.1	说明
主体	5.6.3.5.2	资源定义
主体	5.6.3.5.3	资源标准方法
主体	5.6.3.5.3.1	PUT
主体	5.6.3.5.3.2	DELETE
主体	5.6.3.5.4	资源自定义操作
主体	5.6.4	没有相关资源的自定义操作
主体	5.6.5	通知
主体	5.6.5.1	A. 概况
主体	5.6.5.2	事件通知
主体	5.6.5.2.1	说明
主体	5.6.5.2.2	操作定义
主体	5.6.6	数据模型
主体	5.6.6.1	A. 概况
主体	5.6.6.2	结构化数据类型
主体	5.6.6.2.1	导言
主体	5.6.6.2.2	MLModelMonitorReg型机车
主体	5.6.6.2.3	MLModelMonitorSub型机车
主体	5.6.6.2.4	MLModelMonitorNotify型机车
主体	5.6.6.2.5	MLModelAccuracyInfo型机车
主体	5.6.6.2.6	AnalyticsFeedback型机车
主体	5.6.7	处理错误
主体	5.6.7.1	A. 概况
主体	5.6.7.2	协议错误
主体	5.6.7.3	应用程序错误
主体	5.6.8	特性谈判
主体	5.6.9	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

文稿	章节	标题
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 Nnwdaf_MLModelMonitor:登记/登记/通知/准确的反馈; 严格按端点隔离 TLS，身份与 符号主题绑定；外部攻击者、恶意消费者、被攻陷 TLS终结代理必须分成明确独立配置。精度是 不透明数据，不证明数值正确性。

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	NF项请求的认证	载有MTLF的NWDAF份申请得到保证,其接受的每份登记、订阅或通知都来自请求中提及的NF个实例; 包含AnLF的NWDAF号协议也得到同样的订阅保证。	请求通过相互认证交换TLS介于NF消费者和生产者TS33.50113.4.1.1.2,s0472;TS33.5015.9.2.1),符号主体必须匹配NF实例ID输入TLS客户端证书(E)s0480).	s0004, s0022, s0023, s0472, s0480

ID	简称	对象	文稿怎么说	出处
A03	通知值与订阅值相符	载有MTLF的NWDAF型飞机得到保证,notifCorrId、modelIds和经接受的通知的有效载荷与它所产生的订货相符; 载有AnLF的NWDAF型飞机的订阅与登记相符。	通知必须载有订货的notifCorrId和IDs型号(s0076、s0122、s0126); mLEvent、mLEventFilter和tgtUe的数值应与登记值(s0319)相符。	s0076, s0122, s0126, s0319
A04	每项创建的不同资源	密码NWDAF包含MTLF指定一个不同的registrationId每一登记,以及NWDAF包含AnLF一个不同的subscriptionId每一接受的订阅; 两项接受从来不是一项请求的两次交付。	制作人创建新的注册,并分配registrationId(s0049,s0050,s0051)或新订阅和subscriptionId(s0085,s0086,s0087).	s0049, s0050, s0051, s0085, s0086, s0087
A07	consumerId 符合经认证的消费者	载有MTLF的NWDAF人得到保证,请求机构内的consumerId或consumerSetId确定了NF个经认证的例子,i。 e. 和TLS客户证书身份。	机身搭载了NF型ID型或NF型的ID型机车(s0040,s0041,s0042型机车); 制作人根据TLS客户证书(s0480)和发行商,观众和范围(s0474,s0482,s0485)对象征性主体进行检查.	s0040, s0041, s0042, s0480
A08	通知属于较早的订阅者	密码NWDAF包含MTLF兹保证,接受的通知将受它早先与该消费者订立的订阅书的约束:notifCorrId,则notificationUri页:1modelIds属于该订阅, 操作由符号范围覆盖。	订阅载有modelIds、notificationUri和notifCorrId(s0073、s0075、s0076); 该通知与notifCorrId相呼应,为订阅型号(s0122、s0123、s0126)搭载了modelAccuInfos/anaFeedbacks。	s0073, s0075, s0076, s0122, s0126
K01	长期密钥保密	NRF的令牌签名密钥,NRF与制作方共享的密钥,以及其他端点的TLS密钥,都保存在网络攻击者和持有自己证书的恶意NF处.	用数字签字或NRF(s0405、s0475)中的MAC00来保管托肯; NRF和制作人共享证书(s0439); NF通信受到相互认证的TLS(s0472)的保护.	s0405, s0439, s0475, s0472
K02	准确性和反馈保密性	所监测的准确性信息、分析反馈和UE目标信息仅见于订阅的2个NWDAF例,而不是其他NFs或网络攻击者。	modelAccuInfos财务报告和财务报告anaFeedbacks(b) 通知中载有的(s0125,s0126和(a)和(b)tgtUe登记和订阅s0047,s0083);NF通信是保密的TLS(s0472,TS33.501X.6).	s0125, s0126, s0047, s0083, s0472
D01	通知的真实性和完整性	载有MTLF的NWDAF型飞机得到保证,接受的通知是由载有AnLF的订货的NWDAF型飞机发出的,其中装有notifCorrId型飞机及其发送的有效载荷。	通知是:HTTPPOST页:1notificationUri携带notifCorrId和准确性/反馈有效载荷s0122,s0123,s0126);OAuth2不适用于通知行动(s0412因此,真实性取决于运输会话本身(s0472).	s0122, s0123, s0126, s0412, s0472
Z01	每个请求都带有有效的符号	载有MTLF的NWDAF和载有AnLF的NWDAF保证,他们接受的每一项服务请求都携带一个由允许的NRF所发行的代币,未过期,受众与这名制作人相匹配,范围涵盖业务.	OAuth2 凭客户证书许可,可批准API(s0344,s0345),并由制作人核查签发人,签名,受众,范围和有效期(s0474,s0475,s0482,s0485,s0487); 通知行动位于OAuth2(s0412)之外。	s0344, s0345, s0450, s0474, s0485, s0487, s0412
Z03	与呼叫者绑定的托肯主题	制作人可以放心,它所接受的代币是发给呈递方的:主体符合TLS客户证书身份,受众是这个制作人以及这次操作的范围,主体是consumerId.	制作方检查发行方(s0474),主体对照直通通信案中的TLS客户证明(s0480),受众(s0482),范围(s0485)和过期(s0487).	s0474, s0480, s0482, s0485, s0487
Z05	无法获得其他NF资源	持有自己证书和信物的恶意NF不能读取或更改其他NFs的注册和订阅,不能向另一个NF的notificationUri发布通知,终止代理的TLS在一个链接上失密并不能暴露其他端点的TLS会议.	API规定了整个服务的单一服务级别范围(s0347); TS 29.501警告说,仅服务一级范围就为所有允许的消费者提供所有业务(s0397); 当事人必须信任处理其信息(s2921)的SCP人。	s0347, s0397, s0485

ID	简称	对象	文稿怎么说	出处
U01	反馈绑定在建模和订阅上	载有MTLF的NWDAF号通知(anaFeedbacks:modelIds,事件)的解析反馈来自NWDAF号通知,其中包含AnLF的订阅内容,并参考了该订阅的模式.	anaFeedbacks携带用于行动的IDs和modelIds分析仪(s0328),并在通知中携带notifCorrId(s0122,s0126)的行程; 该通知对订户(s0076)的notifCorrId作了回应。	s0122, s0126, s0076, s0328
U02	外部对已损坏的中介	通知完整性和订阅约束对网络攻击者和持有一个网络的简单文字的攻击者分别进行回答。TLS终止代理(E)SCP上 上 上 上AnLF-MTLF链接。	OAuth2不适用于通知业务(s0412),当使用SCP(s2873)时,消费者和生产者之间没有相互认证; 所有通过SCP通信的当事方都必须信任它(s2921)。	s0412, s0472
U03	NF 笔跨资源	持有自己有效标志的恶意法律NF是否可以操作其他NFs的注册,订阅或通知,以及这一空白是否在规格文本中,还是留待地方政策处理.	API只定义了服务级别范围(s0347),而资源和业务级别范围是可选的,留给API组(s0394); 生产厂商只检查范围是否与操作(s0485)相符。	s0347, s0394, s0397, s0485
X01	通知重播保护	NWDAF包含MTLF的保险保证,它所接受的重复通知是其生产者的新通知,而不是中间人或网络的重播。	NF基于服务的发现、登记和请求交换应支持保密、完整性和回放保护(TS 33.501 5.9.2.1、s2865); JWS(s0405)保护该标志; HTTP/2超过TLS使用(s0149).	s0405, s0122

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 35 段，没选 363 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	它们描述了RFC安全考虑的范围,并指出了一份单独的威胁示范文件; 协议中没有任何财产
P003 至 P004	rfc6749:2790-2809	Z01, Z03	
P005 至 P006	rfc6749:2811-2823	不在范围内	它们是关于授权代码和基于URI的客户端认证; API只使用客户证书发放(s0393)
P007 至 P010	rfc6749:2827-2850	Z03, A07	
P011	rfc6749:2859-2865	K01, Z01	
P012	rfc6749:2867-2868	不在范围内	它涉及隐性赠款,API没有使用。
P013	rfc6749:2870-2872	K01, Z01	
P014	rfc6749:2874-2877	Z03	
P015	rfc6749:2879-2881	Z03, A07	
P016 至 P021	rfc6749:2885-2917	不在范围内	它们涉及新鲜的象征物; 此处使用的客户证书补助金没有发放

段落	出处	定为	不选的原因
P022 至 P029	rfc6749:2921-2980	不在范围内	它们涉及授权代码和重定向URIs, API号没有使用。
P030 至 P033	rfc6749:2984-3003	不在范围内	它们涉及资源所有者密码证书的发放,API没有使用
P034 至 P035	rfc6749:3013-3019	K02, D01, Z05	
P036	rfc6749:3023-3028	A02	
P037 至 P039	rfc6749:3032-3041	Z01	
P040 至 P042	rfc6749:3045-3066	不在范围内	它们涉及对资源拥有者的钓鱼; 客户证书赠款中没有资源拥有者
P043 至 P048	rfc6749:3070-3110	不在范围内	它们涉及基于浏览器的客户端的跨站点伪造请求; NF 客户端不是浏览器
P049 至 P050	rfc6749:3119-3138	不在范围内	点击劫持涉及用户代理商, 而这 API 并不涉及
P051 至 P052	rfc6749:3142-3150	没有陈述目标	关于授权服务器错误处理中的输入验证的建议; 它说没有可以检查的关于这API的财产。
P053 至 P054	rfc6749:3154-3167	不在范围内	它们涉及浏览器流中的打开方向器
P055 至 P062	rfc6749:3170-3210	不在范围内	它们涉及滥用隐含赠款中的代币,此处不使用。
P063	ts-33-501:2491-2491	证明器问不了	竞价降价攻击取决于对算法和安全特征的谈判,而象征模式并不代表
P064 至 P072	ts-33-501:2495-2511	不在范围内	它们涉及UE和NAS以上的服务网络认证,不在API的分流范围。
P073 至 P074	ts-33-501:2515-2517	不在范围内	它们涉及AS和NAS的关键长度,不在API分流范围。
P075 至 P213	ts-33-501:2523-2853	不在范围内	UE型、gNB型、ng-eNB型、SEAF型、UDM/SIDF型、AUSF型和UDR型机车的无线电和订阅安全所需经费,其中没有一台用于API次流量。
P214	ts-33-501:2859-2859	Z05	
P215	ts-33-501:2865-2865	X01, Z01	
P216	ts-33-501:2867-2867	Z01	
P217	ts-33-501:2869-2869	不在范围内	它要求将一个信任域的地形从另一个信任域中隐藏起来,这涉及PLMN之间的部署,而不是PLMN API内部的部署。

段落	出处	定为	不选的原因
P218	ts-33-501:2871-2871	A02, Z03	
P219	ts-33-501:2873-2873	A02, D01, Z05, `scp_compromised`	
P220	ts-33-501:2875-2875	A08, D01	
P221 至 P227	ts-33-501:2879-2891	Z01, `network`	
P228 至 P234	ts-33-501:2895-2907	不在范围内	这些要求是安全理事会的安保要求。NEF面向应用程序函数,此功能API不转弯
P235 至 P239	ts-33-501:2911-2919	Z05, `scp_compromised`	
P240	ts-33-501:2921-2921	Z05, D01, `scp_compromised`	
P241	ts-33-501:2923-2923	没有陈述目标	这是关于把3gpp-Sbi-Originating-Network-Id头装入SCP的规则; 它说,这API号财产中没有任何财产可以检查。
P242 至 P254	ts-33-501:2929-2953	不在范围内	它们涉及核心网络之间的互联,在这个内部的PLMN API之外
P255 至 P312	ts-33-501:2957-3075	不在范围内	它们涉及到SEPP,漫游和互联保护, 在分析的子流之外
P313 至 P318	ts-33-501:3079-3091	不在范围内	他们关心的IPUPS财务报告和财务报告NF四. 区域间所需经费PLMN流量,在此子流量之外
P319 至 P327	ts-33-501:3097-3115	不在范围内	它们涉及信号监测和监测数据的流化,这是单独的功能。
P328 至 P337	ts-33-501:3121-3141	不在范围内	它们涉及操作员的安全可见度和网络的可配置性,而不是这个API的财产.
P338 至 P369	ts-33-501:3149-3215	证明器问不了	它们是密码学和完整性算法识别符和算法选择要求; 原始人的力量在可以问到的 证明器之外
P370 至 P375	ts-33-501:3219-3231	不在范围内	5G-RG型和NSSAAF型,在这一小流量之外
P376 至 P380	ts-33-501:6540-6548	不在范围内	它们涉及N3 用户-飞机接口

段落	出处	定为	不选的原因
P381 至 P385	ts-33-501:9656-9666	不在范围内	它们涉及UE认证的EAP-TLS种变体
P386 至 P394	ts-33-501:10893-10917	不在范围内	它们涉及IAB节点及其接口
P395 至 P396	ts-33-501:11439-11443	不在范围内	它们涉及MBSF和MBSTF职能。
P397 至 P398	ts-33-501:11899-11901	不在范围内	NEF的安全要求 API没有通过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 37 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 13 项，没设的 24 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	含 AnLF 的 NWDAF	参与方	`malicious_nf`	
S02	含 MTLF 的 NWDAF	参与方	`malicious_nf`	
S03	NRF	参与方	按定义全部失守	NRF是授权服务器; 如果攻击者是NRF 这里要求的每一个象征性财产 都从定义上消失 并且文件都问不到他们
S04	外部攻击者	参与方	攻击者得不到更多	外部攻击者是网络上的攻击者,分析中已经出现
S05	恶意合法 NF	参与方	`malicious_nf`	
S06	其他合法 NF	参与方	`malicious_nf`	
S07	被攻陷的 TLS 终结代理	参与方	`scp_compromised`	
S08	外部网络攻击者	参与方	攻击者得不到更多	外部网络攻击者是网络上已经存在的攻击者
S09	被攻陷的 TLS 终结代理或 SCP	参与方	`scp_compromised`	
S10	NF 实例身份	值	攻击者得不到更多	NF例身份由NRF号通过发现公布
S11	服务名 nnwdaf-mlmodel监测器	值	攻击者得不到更多	服务名称在每次请求中都是公开的 URI
S12	modelId / modelIds	值	攻击者得不到更多	ML型号识别器不是秘密的; 所询问的财产是协议,而不是保密
S13	notifCorrId	值	攻击者得不到更多	关联标识符由订阅者创建,仅通过自己的TLS链接进行旅行; 持有它不会让攻击者以制片人的身份说话
S14	notificationUri	值	攻击者得不到更多	通知 URI 是用户端点的地址,不是秘密
S15	mLEvent、mLEventFilter、tgtUe	值	按定义全部失守	如果攻击者已经掌握了目标 UE信息 保密问题由假设本身解答
S16	registrationId	值	`malicious_nf`	
S17	subscriptionId	值	`malicious_nf`	

ID	参与方或值	类别	攻击者条件	不设的原因
S18	consumerId / consumerSetId	值	攻击者得不到更多	consumerId和consumerSetId是NRF号机公布的身份; 2. 要求的财产是被捆绑在经认证的消费者身上,而不是秘密的。
S19	令牌 主体、发行者、听众	值	攻击者得不到更多	每个制片人都会阅读一个符号的主题、发行人和观众,并将该符号提交给
S20	TLS 客户端证书身份	值	攻击者得不到更多	编号NF实例ID输入TLS客户端证书是该证书的公开身份NF
S21	modelIds	值	攻击者得不到更多	IDs型号不是秘密的; 所询问的关于他们的财产与认购协议一致
S22	令牌 镜	值	攻击者得不到更多	范围是一个公共服务名称,用符号标注
S23	NRF 令牌签名私钥	值	按定义全部失守	与NRF签名密钥 每一个令牌都可以被伪造, 因此这里要求的所有令牌属性都会被定义丢失 ; @ info: whatsthis 这些文件都问不到攻击者
S24	NRF 与生产者共享对称密钥	值	按定义全部失守	根据定义,可铸造NRF-生产者共享的关键符号; 这些文件都问不到攻击者
S25	各端点 TLS 会话密钥	值	`scp_compromised`	
S26	modelAccuInfos	值	按定义全部失守	所监测的准确性信息正是要求保密的价值; 一个拥有它的攻击者已经赢得了这个权利
S27	anaFeedbacks	值	按定义全部失守	反馈正是要求保密的值
S28	tgtUe	值	按定义全部失守	目标UE信息正是要求保密的价值
S29	访问令牌	值	攻击者得不到更多	该证书是无记名证书,但生产者对照TLS客户证书身份(s0480)检查其对象; 在攻击者自己的TLS会话上 展示的赃物被拒绝 模型显示
S30	令牌 主体、听觉、镜	值	攻击者得不到更多	主题、受众和范围由制作人根据每项请求阅读。
S31	consumerId	值	攻击者得不到更多	consumerId是消费者的公开身份
S32	各 NF 的注册与订阅资源	值	`malicious_nf`	
S33	TLS 会话	值	`scp_compromised`	
S34	消费者身份	值	攻击者得不到更多	消费者身份是TLS证书中载有的公众NF个实例身份和标志。
S35	通知载荷	值	按定义全部失守	通知有效载荷是要求保密和完整性的价值; 持之以恒的假设回答问题
S36	订阅与注册资源	值	`malicious_nf`	
S37	注册与订阅资源	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`	其自己的NF个实例身份,其自己的TLS个身份证明,以及运行前获得的由NRF为nwdaf-mlmodelmonitor范围签发的有效访问令牌.	API只界定了服务级别的范围,因此,每个获准获得服务的消费者都可以援引其所有服务业务(s0347,s0397); 令牌对象与TLS证书(s0480)核对,所以攻击者没有其他NF的身份.	s0347, s0397, s0480, s0485

攻击者	持有什么	依据	出处
scp_compromised	TLS连接的平面文字和关键材料在AnLF-MTLF链接上终止,从它受损之时起,即订阅后和通知前.	所有通过SCP号通信的当事方都需要信任SCP号通信,以正确处理传递的信息(s2921); 消费者和生产者之间没有通过SCP(s2873)间接通信进行相互认证。	

ID	network	malicious_nf	scp_compromised
A02	成立		
A03	成立		
A04	成立		
A07	成立	不成立	
A08	成立	成立	成立
K01	成立	成立	
K02	成立	成立	不成立
D01	成立	成立	不成立
Z01	成立		
Z03	成立	不成立	
Z05	成立	成立	成立
U01	成立	成立	
U02	成立		不成立
U03	成立	不成立	
X01	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：
46	A02, A03, A07, A08, K01, K02, D01, Z01, Z03, Z05, U01, U02, U03	plain_primitives, many_sessions	所有目标仅依靠普通原始物:TLS作为私人每页密钥下的认证保密通道的模型,作为NRF号的签名的接入符,以及有效载荷的同步认证加密. 该模式涵盖每个角色的无限制会议次数,因此协议,保密和注射式的答案都是关于任何会议次数的. TLS握手本身不是模拟:没有关键确认和记录,这就是A04和X01的重播问题依赖于模型的原因.
46	A04, X01	其他项目	A04和X01询问是否可以两次接受一项请求或通知。 该财产依赖于TLS记录层的重播保护,该模型由单音增长的请求非单音表所代表; ProVerif超近表,所以一个重复的nonce在模型中仍然被接受,尽管协议的运输拒绝.

分析员的结语

所有15个目标都在为它们设定的每个攻击者下得到答复。 登记、订阅和通知、NRF人和网络以外的两名攻击者(一个带有自己证书的恶意NF,一个终止AnLF-MTLF链接的代理的TLS)的进入式发售模式是模拟的。 pv; (中文(简体)). 没有目标基于一个变化的值,所以没有界限。 页:1

为网络和恶意的NF证明:NF个实例认证每次接受,关联识别符和模式约束其订阅,与TLS客户端证书匹配的标语标语,准确性和反馈的保密性,通知的真实性,标语检查,连接被破坏的代理的隔离并不终止,其他实例的资源识别符的不确定性. 对有故障变体

(a02_reg_ctl,a02_sub_ctl,k01_tlskey_ctl,z05_regid_ctl,z05_corr_ctl,d01_ctl,k02_ctl,x01_ctl)的证明进行了记录控制.

规格文本的一个漏洞:consumerId的注册从未与经认证的消费者相比,因此,任何在另一个情况下持有自己注册的有效标志的事例都是consumerId(a07_body_nf,malicious_nf之下). 关闭它的变化 被检查的固定消费者。 pv:攻击查询变为验证,运行存活,没有其他记录的答案变化.

记录的已知结果转载如下:准确度和反馈有效载荷可读,可重写为受损的SCP,可以两次发送通知,确切地说,TS 33.501是SCP信托,OAuth2是不适用通知的。

其余的是什么:A04只在其识别-注入读数中回答; 其请求-重播读数在模型中被伪造,因为ProVerif超近请求非ces的表,一个每个连接-ticket的变体丢失了正常运行. 过期,吊销,资源级授权,consumerSetId和TLS握手本身均在模式之外,如限额所列.