

作业 2

到期日:墨尔本时间 2025 年 5 月 1 日星期四晚上 11:59

介绍

这份讲义是作业2的作业表。该作业占总成绩的20%。  
将以与作业 1 相同的方式完成作业,除非你被分配  
如果你的伴侣不再关注这个话题,就换一双新的。  
在此作业中,您将使用 Alloy 来诊断和修复安全音频通话中的漏洞  
软件包。此漏洞的灵感来自于  
Signal 是一款端到端加密消息应用程序(现已修复),可在多种平台上运行  
流行平台包括iPhone、Android、台式电脑等。  
我们将在本次作业中考虑使用音频呼叫协议的简化版本。具体来说  
实际协议使用多种网络传输机制,并区分不同的呼叫建立阶段,包括信令和媒体传输。然而,在本作业中,我们将考虑  
一个简单的协议,其预期的交互顺序如图 1 所示。

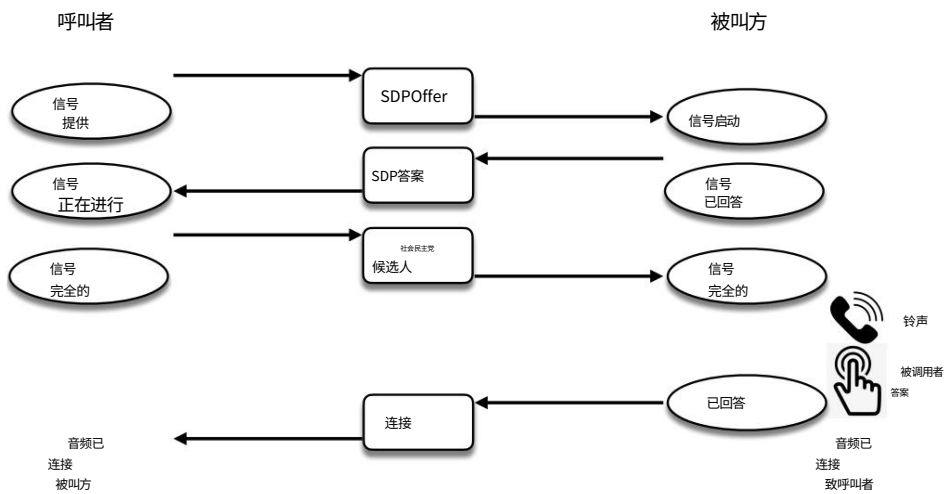


图 1:协议中预期的交互序列。

对于此任务,我们将忽略视频媒体,并假设通话仅传输音频  
参与者之间。  
我们将发起呼叫的一方称为呼叫者,将接收呼叫的一方称为  
呼叫者作为被呼叫者。图中的椭圆代表每一方在不同时间所处的不同状态  
通话过程中的点。圆角矩形表示交换的消息  
两位参与者之间。  
呼叫者首先向被呼叫者发送一个 SDPOffer 消息,这样呼叫者就移动  
进入 SignallingOffered 状态。当被叫方收到 SDPOffer 消息时,他们进入

SignallingStart 状态。从此状态开始,被叫方发送一条 SDPAnswer 消息,并进入 SignallingAnswered 状态。当主叫方收到此消息后,主叫方进入 SignallingOngoing 状态。从此状态开始,主叫方向被叫方发送一条 SDPCandidates 消息,并进入 SignallingComplete 状态。当被叫方收到此消息后,被叫方也进入 SignallingComplete 状态。

此时,双方已交换了足够的信息,允许音频在彼此之间传输。因此,被叫方的设备(例如手机)开始响铃,告知对方有来电。当被叫方接听电话(例如按下手机上的按钮)时,他们将进入“已应答”状态。在此状态下,被叫方会向呼叫方发送“连接”消息,然后被叫方会将其音频设备连接到呼叫方(即开始向呼叫方传输手机麦克风录制的音频)。呼叫方收到此“连接”消息后,也会将其音频设备连接到被叫方,此时双方可以交换音频。

正式模型:本作业将提供该协议的部分合金模型。你的部分任务是使用上述描述和以下信息完成该模型。

Alloy 模型正式描述了协议中参与者的状态。我们将该参与者称为 User。消息在参与者地址之间发送。用户的地址为 UserAddress。每条消息包含一个源地址和一个目标地址,以及一个消息类型字段(例如上文中的 SDPOffer 等)。

Alloy 模型还描述了网络的状态,具体来说,通过记住参与者之间在网络上发送的最后一消息。

用户的 Alloy 模型会记住用户决定呼叫的最后一个参与者(当用户作为呼叫者时),以及用户决定接听的最后一个参与者(当用户作为被呼叫者时)。我们将这两条信息称为“最后被呼叫者”和“最后被呼叫者”。

最后回答。

对于每个地址,它还会记住该地址的呼叫(如果有)的状态(例如 SignallingOffered、SignalingAnswered 等)。

用户发送的消息的源地址设置为 UserAddress。其 dest 字段设置为消息发送目标参与者的地址。

发送消息会将其放入网络。初始 SDPOffer 消息只能发送到最后被呼叫的地址(即其目标地址必须是最后被呼叫的地址),并且仅当用户没有记录该地址的呼叫状态时才可以发送。

只有当消息的目标地址为 UserAddress 且该消息当前在网络上时,用户才能接收该消息。接收消息会将其从网络中移除。只有当消息的源地址(即呼叫者)没有记录呼叫状态时,才能接收 SDPOffer 消息。

其他消息仅当用户记录的消息目标地址的呼叫状态如图 1 所示时才可发送(例如,只有当用户在该地址的呼叫状态为 SignallingStart 时,才能向该地址发送 SDPAnswer)。同样,仅当用户记录的消息源地址的呼叫状态如图 1 所示时,才能接收消息(例如,只有当用户在该地址的呼叫状态为 SignallingStart 时,才能从该地址接收 SDPAnswer)。

当用户对该地址的呼叫状态为 SignallingOffered 时)。

发送消息会改变用户在消息目标地址的呼叫状态,如图 1 所示 (例如,当用户发送 SDPAnswer 消息时,目标参与者记录的用户呼叫状态会更改为 SignallingAnswered)。同样,接收消息会改变用户在消息源地址的呼叫状态,如图 1 所示 (例如,当用户收到 SDPAnswer 消息时,消息源 (发送者)记录的呼叫状态会更新为 SignallingOngoing)。

只要用户记录的该源地址的呼叫状态为 SignallingComplete,就可以从任何源地址接收 Connect 消息。

当用户发送或接收消息时,系统的任何部分都不会发生变化,但以下情况除外:

- 网络 (发送消息会将其添加到网络;接收消息会将其删除 (来源于网络))
- 用户为相关参与者录制的通话状态 (消息的来源或目的地,取决于用户是接收还是发送),

并注意以下例外情况:

- 接收 SDPCandidates 消息会导致振铃状态更新,以引用消息的源地址 (即呼叫者的地址)。
- 发送 Connect 消息会导致音频连接到消息的目的地 (即对呼叫者而言)。
- 类似地,接收 Connect 消息会导致音频连接到消息的源地址。

Alloy 模型还包含一些操作,分别用于模拟用户决定接听正在响铃的电话以及决定呼叫其他参与者的情况。这些操作分别更新状态中的“最后接听”和“最后呼叫”部分。

攻击者 Alloy 模型还包含潜在攻击者的行为。攻击者控制 (拥有)的地址集合称为 AttackerAddress。用户唯一可以交互的其他参与者是潜在攻击者,即 AttackerAd-address 集合中的地址。

攻击者可以将任何消息发送到源地址为 AttackerAddress 地址的网络上。他们无法执行任何其他操作,也无法修改系统中的任何其他状态。

## 你的任务

任务 1:完成初始模型;寻找攻击 (8 分)

你的首要任务是完成模型中缺失的部分。这需要你仔细理解给定的模型,以便找到如何填补缺失部分的方法。

在本次作业期间,您不应添加任何额外的 sig 声明,也不应修改任何现有的 sig 声明。

1. [5 分] 完成用户接收后谓词以完成初始模型。 -
2. [2 分] 如上所述,该协议存在一个漏洞。具体来说,攻击者可以导致用户处于这样一种状态:他们的音频已连接到攻击者,但用户尚未决定是否呼叫该攻击者或接听该攻击者的呼叫。

写一个合金断言,断言没有坏状态,断言这种情况永远不会发生。

3. [1 分] 使用 Alloy 发现此漏洞。请在生成此断言反例的检查命令上方的注释中描述该漏洞。也就是说,描述原始协议存在哪些问题以及漏洞行为是如何产生的。

## 任务 2:修复模型 (4 分)

1. [2 分] 为协议设计一个最小的修复方案,以修复漏洞。这是你能想到的最小改动,能够在不改变协议预期功能的情况下,消除漏洞。

在 Alloy 文件底部添加一条注释,描述您如何修复漏洞以及更改了哪些部分。

您不需要向任何消息添加任何额外的消息、签名或任何额外的信息来实现此处建模的协议的最小修复。

2. [2 分] 证明你的“无坏状态”断言现在成立。使用合适的上限在进行此项检查时。

添加注释来证明/解释您所选择的界限,以及具体来说,您认为该检查提供了哪些保证。

为了获得满分,我们希望您选择一个足够大的边界,以提供一些真正的保证,但又不能大于获得这些保证所需的范围。您需要仔细思考您的边界意味着什么,例如,该边界涵盖了哪些行为,以及为什么证明所有这些行为都不存在攻击就能保证协议的有效性。

如果您认为您选择的界限不能提供良好的保证,您应该这样说并解释原因。

## 任务 3:模型检查 (8 分)

你的固定模型应该能够模拟用户作为被调用者或调用者的协议执行。它还应该支持其他合理的执行轨迹。

Alloy 文件中提供了一个示例谓词(成功运行),以动画形式呈现用户发起呼叫(即,呼叫者)的行为。

1. [2 分] 研究 finally 关键字和给定的 successful run 谓词的语义。然后定义一个等效的谓词 successful run2,它不使用 finally 关键字。

2. [2 分] 写一个名为 “equivalent”的断言,验证 “成功运行”和 “成功运行2”完全等价。请使用适当的界限来检验此断言。

注意:不要修改原来的成功运行谓词。

3. [4 分] 编写一个谓词 “两次响铃”,并使用 Alloy 的 run 命令探索用户为一个呼叫者响铃,然后立即为另一个呼叫者响铃的协议行为。换句话说,应该存在两个连续的状态:第一个状态是用户为一个呼叫者响铃,第二个状态是用户为另一个呼叫者响铃。

提示:充分理解任务 3.1 和 3.2 中的 finally 关键字可能会有所帮助。合适的运行边界对于生成示例至关重要。

## 学术不端行为

大学不端行为政策适用于此作业。鼓励学生讨论作业主题,但所有提交的作业必须体现学生对该主题的理解。

学科工作人员非常重视抄袭行为。过去,我们成功起诉了多名违反大学规定的学生。这些学生通常会导致评估得分为零,有时甚至导致该科目不及格。

## 提交

使用主题 LMS 上的链接提交您的合金文件。

每对学生中只有一名学生应提交解决方案,并且每份提交的解决方案都应清楚地标明两位作者。

逾期提交:逾期提交将按每日10% (2分)扣分。如果您有理由需要延期,请在截止日期前发送电子邮件给Toby进行沟通。

请注意,其他科目在同一日期左右有作业截止并非获得延期的充分理由。学生有责任确保,如果他们有一批作业在同一时间截止,则应尽早开始其中一些作业,以避免在截止日期前后出现瓶颈。