IKE的野蛮模式的消息交换过程是什么?

刘军 2006-10-25 发表

IKE的野蛮模式的消息交换过程是什么?

野蛮模式中,只提供带有一个变换的建议载荷;响应者可以选择接受或者拒绝该建议.DH公开值和随机数据和身份信息也在第一条消息中传送消息2.如果响应者接受发起者的建议,它发送一个SA载荷,其中封装有一个包含发起者的建议和推荐的建议载荷.它将DH公开值需要的随机数据和身份消息作为消息的一部分同时传送.这个消息受到协商一致的认证函数保护.消息3发起者发送应用一致同意的认证函数生成结果.实际上,这个消息认证发起者并且证明它是交换的参与者.这个消息使用前两个消息交换的密钥消息生成的密钥进行加密.但是要注意:包含身份信息的消息未被加密,所以和主模式不同,野蛮模式不提供身份保护.