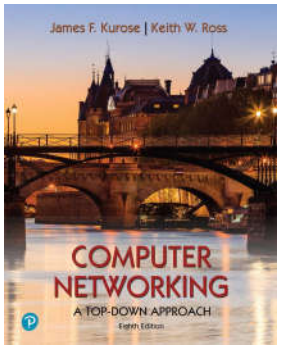
第 8 章
网络安全（下）

中国科学技术大学
自动化系 郑烇
改编自Jim kurose, Keith Ross

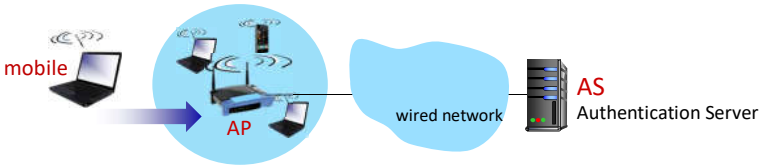


Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

第八章 提纲

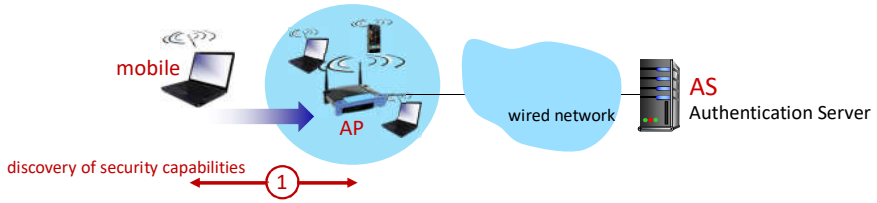
- 什么是网络安全?
- 加密原理
- 认证，报文完整性
- 安全电子邮件
- 使TCP连接安全：TLS
- 网络层安全性：IPSec
- 无线和移动网络的安全
  - 802.11 (WiFi)
  - 4G/5G
- 实践中的网络安全：防火墙和IDS

802.11: 认证和加密



到来的移动设备必须:
- 和AP建立起关联：在无线链路上建立起通信关系
- 被网络认证

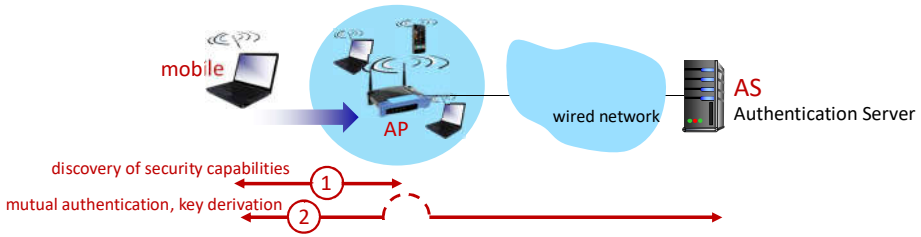
802.11: 认证和加密



① 安全能力的发现:
- AP通告其存在，通告其支持的认证和加密形式
- 设备请求其所希望的认证和加密的方式

尽管这时设备和AP之间已经交换了信息，但是还没有完成认证，没有共享加密所需要的keys

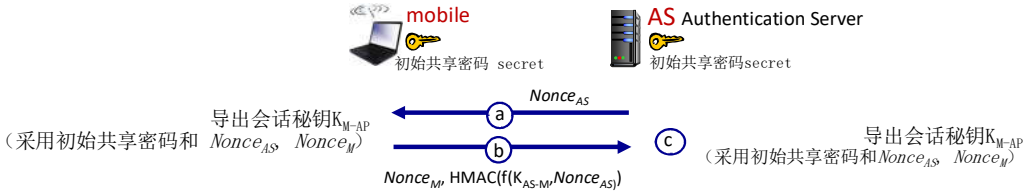
802.11: 认证和加密



② 相互认证，共享对称秘钥生成:

- 前提：AS,移动设备M具备共享的公共密码secret(e.g., password)
- AS,移动设备M采用secret，nonces（防止重返攻击），加密散列（确保报文的完整性） 相互**认证**
- AS,移动设备M导出**对称式的会话秘钥**

802.11: WPA3 握手



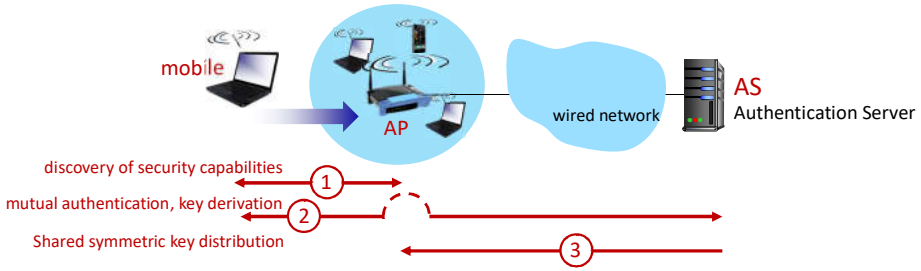
② ⓐAS生成$Nonce_{AS}$，发送给移动设备M

ⓑ 移动设备M接收$Nonce_{AS}$

- 生成$Nonce_M$
- 生成对称式共享会话秘钥K_{M-AP}：*用$Nonce_{AS}$, $Nonce_M$, 和初始会话秘钥如: password*
- 发送$Nonce_M$（*用于AS生成秘钥*）*和*采用 $Nonce_{AS}$ 和secret签署的HMAC(用用于AS验证M的身份)

ⓒ AS导出对称式的共享秘钥 key：K_{M-AP}

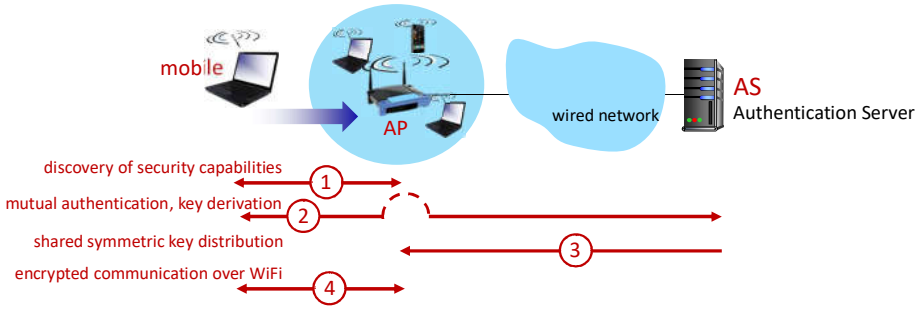
802.11: 认证和加密



③ 共享的对称式会话秘钥分发（e.g., 用于AES加密）

- 在移动设备和AS上，相同的key被导出
- AS通告AP，共享对称式的会话key

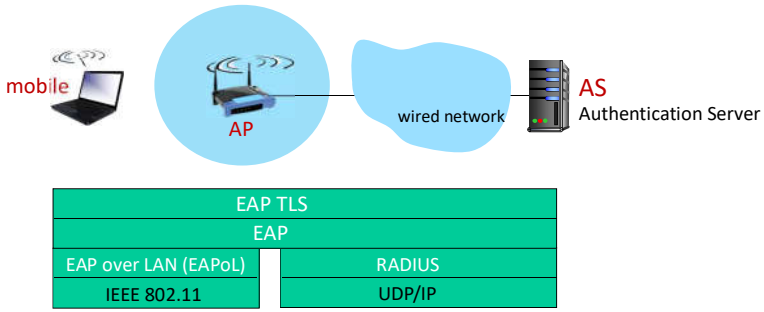
802.11: 认证和加密



④ 在移动设备M和AP之间采用加密方式，与远端主机通信

- 在移动设备和AS之间采用相同的导出秘钥
- AS通告AP该共享对称式的秘钥

802.11：认证和加密



- Extensible Authentication Protocol (EAP) [RFC 3748] 定义了端到端的、客户端(移动节点) 到AS认证服务器的协议

第八章 提纲

- 什么是网络安全?
- 加密原理
- 认证，报文完整性
- 安全电子邮件
- 使TCP连接安全：TLS
- 网络层安全性：IPSec
- 无线和移动网络的安全
  - 802.11 (WiFi)
  - 4G/5G
- 实践中的网络安全：防火墙和IDS

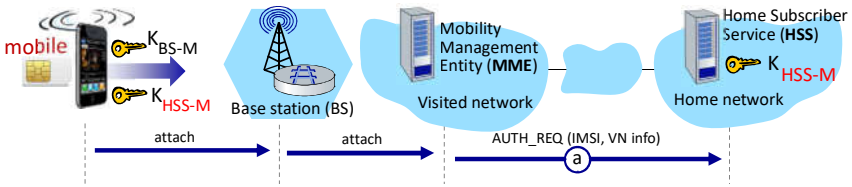
4G LTE中的认证和加密

- 到来的移动设备必须：
  - 和基站BS建立关联：通过4G无线链路通信
  - 双向认证：移动终端被网络认证，以及移动设备认证网络
- 与WiFi明显的差别：
  - 移动设备的SIM卡：提供全局的身份标识，存储了共享keys
    - 全局身份标识有层次
  - 在被访问网络(visited network)中的服务取决于在归属网络(home network)中订购的业务

4G LTE中的认证和加密

- 移动设备、BS采用导出的会话秘钥K_{BS-M}在4G链路上加密通信数据
- 被访网络中的MME+归属网络中HHS，共同扮演了WiFi中AS的角色
  - 最终认证设备是：HSS
  - 被访网络和归属网络之间有着信任关系和商业关联

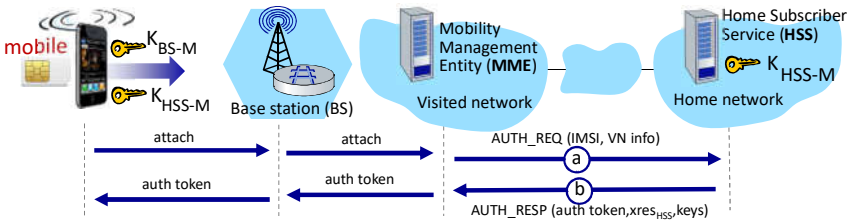
4G LTE中的认证和加密



ⓐ 认证请求发出，到达归属网络的HSS

- 移动设备发送附加报文attach（包括它所在的IMSI-国际移动用户识别码，被访网络的信息VN）从BS中继到被访MME，最终到达HHS
- IMSI有结构，包含了移动终端归属网络home network的标识

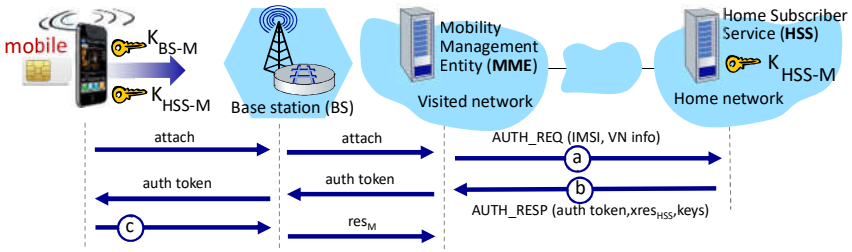
4G LTE中的认证和加密



ⓑ HSS采用预先和移动设备M共享的密码K_{HSS-M}，来导出认证令牌*auth_token*，以及期望认证响应令牌：$xres_{HSS}$

- *auth_token*包含：HSS采用和M共享的secret：K_{HSS-M}加密的信息
- *auth_token*传回M：让移动设备知道谁知道预分配secret，就是谁来计算认证令牌*auth_token*让**移动终端M认证网络**
- 被访网络的HSS（应该是MME？）保持$xres_{HSS}$用于以后使用

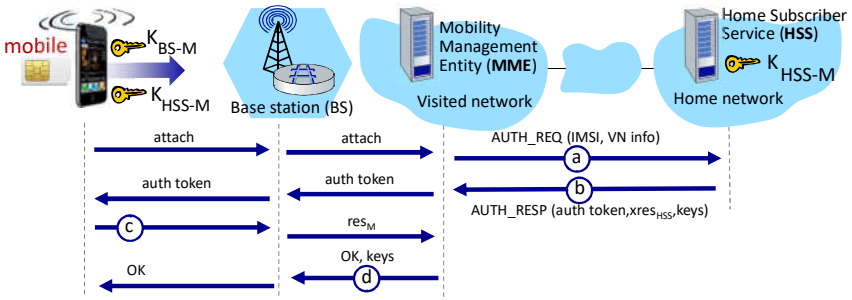
4G LTE中的认证和加密



ⓒ 来自移动终端的认证响应：

- 移动设备采用它保存的secret计算出resM，和在HSS中计算$xres_{HSS}$同样的加密运算
- 将res_M传送给MME

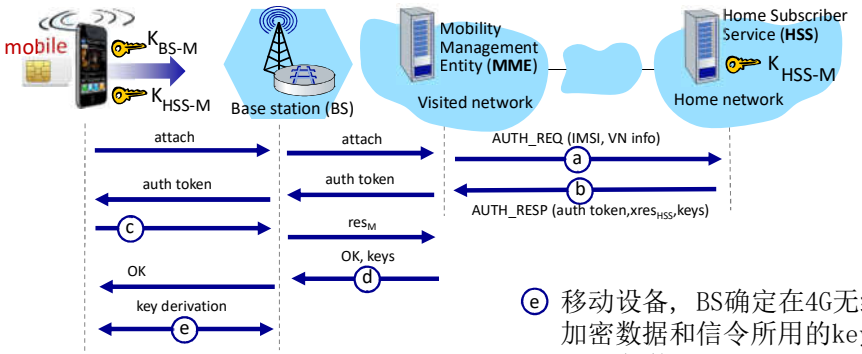
4G LTE中的认证和加密



ⓓ 移动设备被网络认证：

- MME比较移动设备计算的res_M的和HSS计算的$xres_{HSS}$，*如果匹配，**移动设备M被认证通过；***
- MME通知BS：移动设备被认证通过，为BS生成keys

4G LTE中的认证和加密



ⓔ 移动设备，BS确定在4G无线链路中加密数据和信令所用的keys
- 可能使用AES

认证和加密：从4G到5G

- 4G：在被访网络中的MME最终做出认证决定
- 5G：归属网络做出认证决定
  - 被访MME扮演一个“中间人”角色，但是有权拒绝认证

- 4G：采用预先共享秘钥
- 5G：对于IoT设备来说无法具备预共享秘钥

- 4G：设备IMSI被明文传输到BS
- 5G：公开秘钥加密IMSI

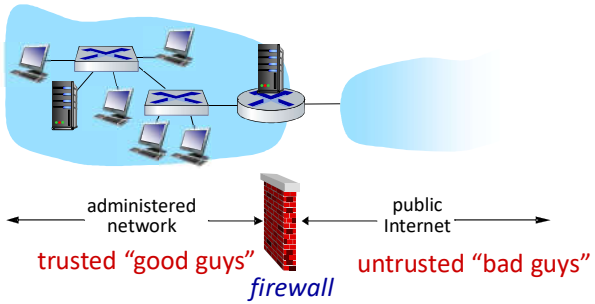
第八章 提纲

- 什么是网络安全?
- 加密原理
- 认证，报文完整性
- 安全电子邮件
- 使TCP连接安全：TLS
- 网络层安全性：IPSec
- 无线和移动网络的安全
- 实践中的网络安全：防火墙和IDS

防火墙

firewall

将组织内部网络和互联网络隔离开来，按照规则允许某些分组通过（进出），或者阻塞掉某些分组



防火墙：必要性

阻止拒绝服务攻击：

SYN flooding：攻击者建立很多伪造TCP连接，对于真正用户而言由于服务器的资源被耗尽，他们的访问被拒绝

阻止非法的修改/对非授权内容的访问

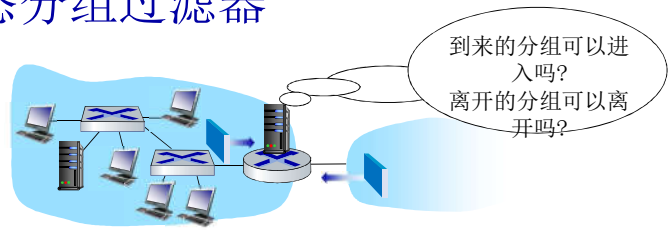
- e.g.，攻击者替换掉CIA的主页

只允许认证的用户能访问内部网络资源（经过认证的用户/主机集合）

2种类型的防火墙：

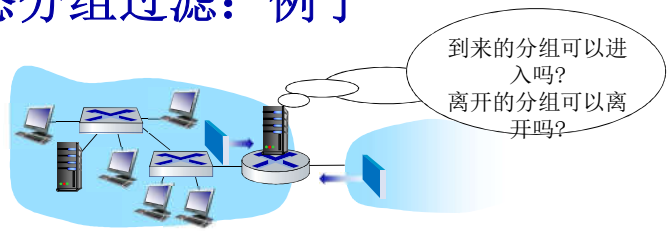
- 无状态分组过滤器
- 有状态分组过滤器
- 应用网关

无状态分组过滤器



- 内部网络通过配置防火墙的路由器连接到互联网上
- 路由器对分组逐个过滤，根据分组相应字段匹配到规则相应自字段来决定转发还是丢弃
  - 源IP地址，目标IP地址
  - TCP/UDP源和目标端口
  - ICMP报文类别
  - TCP SYN 和ACK bits

无状态分组过滤：例子



- 例1:阻塞进出的数据报：只要拥有IP协议字段 = 17，而且源/目标端口号 = 23.
  - 结果：所有的进出UDP流 以及TCP 上telnet连接分组都被阻塞掉
- 例2: 阻塞进入内网的TCP段：它的ACK=0.
  - 结果：阻止外部客户端主动和内部网络的主机建立TCP连接，但允许内部网络的客户端主动和外部服务器建立TCP连接

无状态分组过滤器：更多例子

策略	防火墙设置
不允许外部的web进行访问	阻塞掉所有外出具有目标端口80的IP分组
不允许来自外面的TCP连接，除非是机构公共WEB服务器的连接	阻塞掉所有进来的TCP SYN分组，除非130.207.244.203, port 80
阻止Web无线电占用可用带宽.	阻塞所有进来的UDP分组 - 除非 DNS和路由器广播
阻止你的网络被smurf DoS所利用	阻塞掉所有到达广播地址(130.207.255.255)的ICMP分组.
阻止内部网络被tracerout，从而得到你的网络拓扑	阻塞掉所有外出的 ICMP TTL过期的流量

Access Control Lists

ACL：规则的表格，自动向下和输入的分组进行匹配：(action, condition) 对：有点像OpenFlow 转发表(Ch. 4)！

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

有状态分组过滤

- *无状态分组过滤器：* 重型工具？
  - 防火墙会让“无意义”的分组通过，例如：dest port = 80, ACK bit set
  - 该TCP连接甚至都没建立起来：

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *有状态的分组过滤器：* 跟踪每个TCP连接的状态
  - 跟踪TCP连接建立（SYN），拆除（FIN）：然后才让相应后续分组通过
  - 防火墙上的非活跃连接会超时，不再允许相应的分组通过防火墙

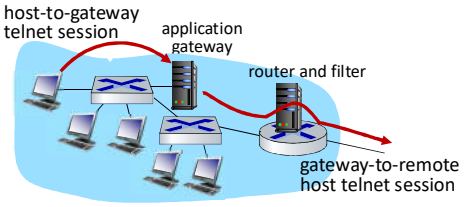
有状态分组过滤

ACL增强：在允许分组通过之前需要检查连接状态表

action	source address	dest address	proto	source port	dest port	flag bit	check connection
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

应用程序网关

- 根据应用数据的内容来过滤进出的数据报，就像防火墙根据IP/TCP/UDP字段来过滤一样
- 例子：允许特定的内部站点登录到外部服务器，但不是直接登录



1. 需要所有的telnet用户通过网关来telnet
2. 对于认证的用户而言，网关建立和目标主机的telnet connection ，网关在2个连接上进行中继
3. 路由器过滤器将所有不是来自网关的telnet分组全部过滤掉

防火墙和应用程序网关的局限性

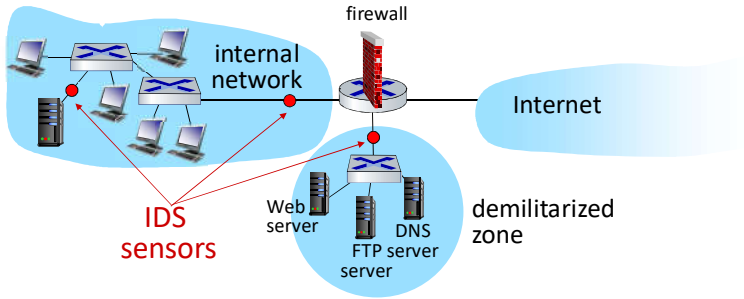
- IP spoofing: 路由器不知道数据报是否真的来自于分组源地址声称的IP
- 应用网关：如果有多个应用需要控制，就需要有多个应用程序网关
- 而且客户端软件需要知道如何连接到这个应用网关
  - e.g., 必须在Web browser中配置网络代理的Ip地址
- 过滤器对UDP段所在的分组，或者全过或者全都不过
- 折中：外部通信的便利性vs安全的级别
- 很多高度保护的站点仍然受到攻击的困扰

IDS：入侵检测系统

- 分组过滤：
  - 对TCP/IP头部字段进行检查
  - 不检查会话分组间的相关性
- IDS: intrusion detection system
  - *深入分组检查:* 检查分组的内容（e.g., 检查分组中的串是否和已知攻击数据库的病毒和攻击的特征码匹配）
  - 检查分组间的相关性，判断是否是有害的分组（时间序列）
    - 端口扫描
    - 网络映射
    - DoS 攻击

IDS：入侵检测系统

- 多个IDSs：不同的网段，放置探针，根据需要进行不同类型的检查



总 结

基本原理
- 加密（对称和公开秘钥加密体系）
- 报文完整性
- 端到端认证（鉴别）

各个层次的安全性
- 安全电子邮件
- 安全传输(TLS)
- IP sec
- 802.11, 4G/5G

网络安全设备：防火墙和IDS