网络安全 – 无线网络安全防护

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

上周回顾

1. VPN的组成
2. 比较PPTP与L2TP
3. 简述IPSec中AH协议的功能
4. 简述IPSec中ESP协议的功能

VPN使用的协议与实现 - PPTP与L2TP比较

网络基础

- PPTP：IP网络
- L2TP：面向数据包的点对点的连接
  - 例如：IP（UDP），虚拟电路、ATM交换电路

隧道

- PPTP：单一隧道，不支持隧道验证
- L2TP：支持多隧道和隧道验证，不同服务质量创建不同隧道

压缩头的开销

- PPTP/L2TP：6/4 byte

VPN使用的协议与实现 - IPSec保护技术 3

Authentication Header (AH)

- AH协议包头可以保证信息源的可靠性和数据的完整性
- 工作原理
  - 发送方将IP包头、高层数据、密钥这三部分通过某种散列算法进行计算，得出AH包头中的验证数据，并将AH包头加入数据包中
  - 接收方将收到的IP包头、数据和密钥以相同的散列算法进行运算，并把得出的结果和收到的数据包中的AH包头进行比较，如果相同，则表明数据在传输过程中没有被修改，并且是从真正的信息源处发出的

VPN使用的协议与实现 - IPSec保护技术 4

Encapsulating Security Payload (ESP)

- **ESP可以提供数据的完整性和可靠性**
- **使用非对称密钥技术**
- **密钥交换采用IKE(Internet Key Exchange)**
  - **IKE不是在网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥，并且即使第三者截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥**

常见攻击与弱点

无线安全对策

无线通信安全

无线VPN

常见攻击与弱点

无线安全对策

无线通信安全

无线VPN

有线网络 vs 无线网络

有线网络

- **光纤是目前传输速度最快的线缆了，而且抗干扰能力强**
- **速度快，可靠**

无线网络

- **4G/5G/6G**
- **利用无线电或者微波在空气中传播**
- **便捷，易被干扰**

无线网络安全

1999年，IEEE发布了802.11标准，定义了无线局域网和无线城域网的介质访问控制层和物理层的规范

只要在访问点范围内，所有无线终端都可以接收到无线信号

WEP (Wired Equivalent Privacy)

为了保证数据能安全地通过无线网络传输而制定的一个加密标准，使用了共享秘钥RC4加密算法。

密钥长度最初为40位，后来增加到128位，有些设备可以支持152位加密。

固有缺陷：

- 一个服务区内的所有用户都共享同一个密钥，一个用户丢失或者泄漏密钥将使整个网络不安全
- RC4算法自身不足，密钥管理没有具体方案

WEP的主要用途

提供接入控制，防止未授权用户访问无线网络

WEP加密算法对数据进行加密，防止数据被攻击者窃听和监听

防止数据被攻击者中途恶意篡改或者伪造

WEP加密算法采用了静态密钥，各WLAN终端使用相同的密钥访问无线网络

WEP同时也提供了认证功能

WEP密钥管理的弱点

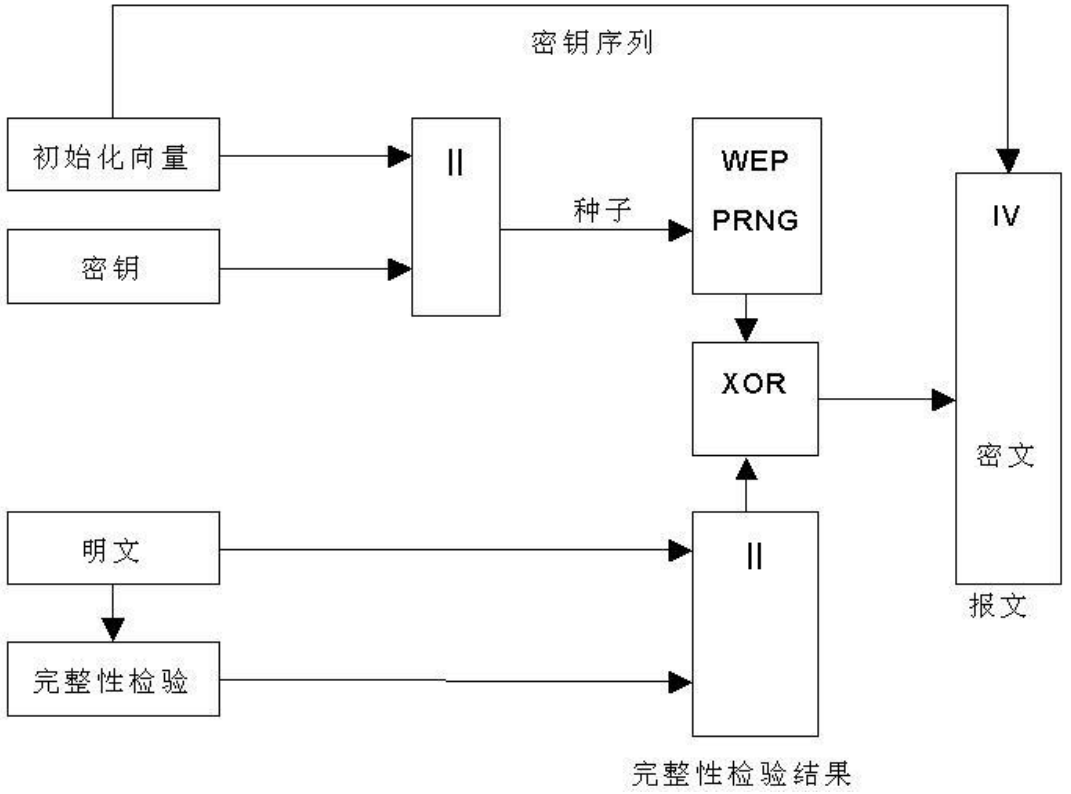
共享密钥如何生成

如何向外分发

如何在密钥泄露后更改密钥

如何定期更新密钥

常见攻击与弱点



常见攻击与弱点 – 搜索

发现目标

- 访问点(AP)、安全集标识符(SSID)

估计目标

- Non-WEP
- WEP：MAC地址(制造商)、SSID、网络名称、厂商的信息(缺省密钥)

破坏目标

- 破解密码算法
- 监听流量

常见攻击与弱点 – 窃听

离源节点距离要比较近

窃听

- Ethereal (www.ethereal.com)
- TcpDump (www.tcpdump.org)
- AiroPeek (www.wildpackets.com)
- 网卡混杂模式

防范

- 交换方式：不采用集线器方式
- 关闭所有网络身份识别的广播功能
- 密码保护：SSH，安全拷贝etc.

常见攻击与弱点 – 欺骗

欺骗(spoofing)

- 欺骗是指攻击者装扮成一个合法用户，非法访问受害者的资源以获取某种利益或达到破坏目的
- MAC地址
- 利用流密钥特证攻击身份验证

构架特点

- 集中式无线网络的核心节点实现认证相对容易
- 分布式无线网络缺少核心节点，多跳传输、移动性等，较为复杂

防范

- 额外身份验证

常见攻击与弱点 – 非授权访问

非授权访问

- **非授权访问是指攻击者违反安全策略，利用安全系统的缺陷非法地占有系统资源，或者访问本应受保护的信息**

防范

- **通信单元增加认证机制**
- **核心节点/移动节点**

常见攻击与弱点 – 接管

接管(hijack)

- 攻击者伪装成合法用户插入会话过程，并继续与其它节点通讯
- 动态ARP、网关
- 欺骗访问点(AP)

防范

- ARP管制
- 静态IP/MAC匹配
- 强化身份验证机制

常见攻击与弱点 - DoS

DoS

- **Ping – IMCP Echo**
- **无线频率 – 传输冲突**
- **大量非法或合法的身份验证请求**

防范

- **调整频率**
- **电磁防护**

常见攻击与弱点 – 其他方法

其它方法

- JavaScript, etc 在线网购的信息泄露

密钥存储

- hack tools
- 介质/设备的偷窃

常见攻击与弱点

无线安全对策

无线通信安全

无线VPN

无线安全对策 – 安全策略 1

安全策略是管理规则的一种格式化描述，是用户在组织内都应该遵循的技术和访问控制的总称

无线环境中的用户，比有线环境中的用户面对着更多的挑战

安全策略必须能够寻址

无线安全对策 – 安全策略 2

AP不广播SSID

- **通过用户端SSID匹配**

算法必须公开，而密码应该谨慎选择

AP漫游安全

- **避免不同空间规则不一致**

坚固的认证和加密

- **验证信道采用VPN**

无线安全对策 – WEP的主要用途

提供接入控制，防止未授权用户访问无线网络

WEP加密算法对数据进行加密，防止数据被攻击者窃听和监听

防止数据被攻击者中途恶意篡改或者伪造

WEP加密算法采用了静态密钥，各WLAN终端使用相同的密钥访问无线网络

WEP同时也提供了认证功能

无线安全对策 - WEP保密性

无加密

40位，128位

24位的IV

关注点

- **位数越长，加密强度越大**
- **避免密钥重用**

WEP验证过程

1. 请求方(客户端)向验证方发送连接请求
2. 验证方(AP)接受请求，并将生成的随机验证内容反传递给请求方，进行响应
3. 当请求方收到验证内容后，利用共享密钥流加密验证内容，随后就返回
4. 验证方解密验证内容，并同原始内容进行比较
5. 如果匹配，请求方就通过了验证

无线安全对策 - ESSID

IEEE802.11b

无线终端访问的服务区域认证ID (ESSID)

在每一个AP内都会设置唯一的网络ESSID

每当无线终端设备要连接AP时，AP会检查其ESSID是否与自己的服务区域认证ID一致

只有当AP和无线终端的ESSID相匹配时，AP才接受无线终端的访问并提供网络服务；如果结果不匹配，访问点就拒绝给予服务

ESSID，SSID，BSSID

SSID包括ESSID，BSSID

BSSID Basic Service Set Identifier

- 一个无线网络至少由一个连接到有线网络的AP和若干无线工作站组成

一位员工于公司内连接无线网络

- BSSID可理解为每个办公室的AP
- 但是整个公司的SSID为xxx公司

无线安全策略 - SSID匹配

通过对多个无线AP设置不同的SSID (Service Set Identifier)标识字符串(最多32个字符)，并要求无线工作站出示正确的SSID才能访问AP，这样就可以允许不同群组的用户接入，并对资源访问的权限进行区别限制。

SSID只是一个简单的字符串，所有使用该无线网络的人都知道该SSID，很容易泄漏；使用SSID只能提供较低级别的安全防护。

如果设备无线网卡上设定其SSID为“ANY”时，它就可以自动的搜寻在讯号范围内所有的存取点，并试图连上它

无线安全对策 – 过滤MAC

过滤接入终端的介质访问控制(MAC)地址，只有经过注册的设备才可以接入到无线网络

方法
- MAC地址控制表
- 过滤的位置

优点
- 方便、直接、第一层防护

缺点
- MAC地址可能泄漏并被伪造
- MAC地址控制表需要更新、查询代价

无线安全对策 – 过滤协议

方法类似于防火墙

- 位置：位于第3、4层（IP，端口）

优点

- 过滤能力强大

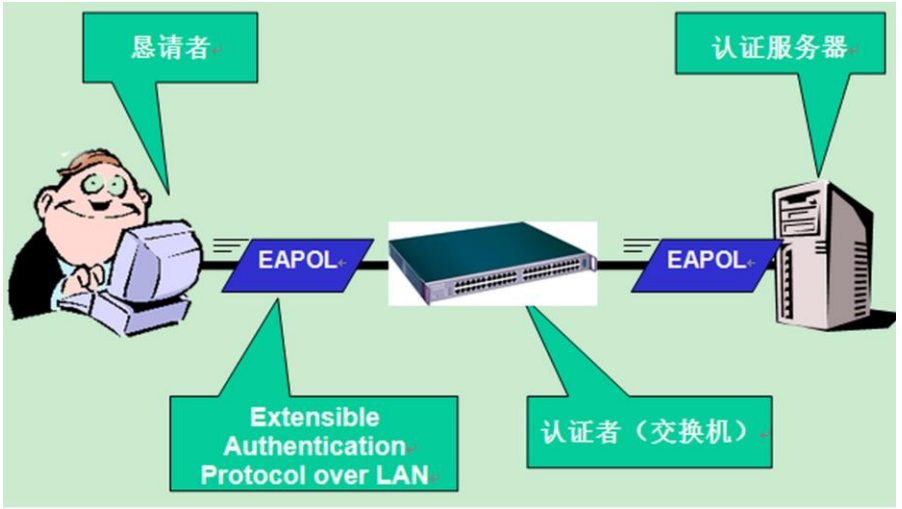
缺点

- 难以合理制定复杂的规则
- 放置位置

无线安全对策 – 端口访问控制技术

需要和扩展认证协议EAP(Extensible Authentication Protocol)配合来实现用户认证和密钥分发。EAP允许无线终端使用不同的认证类型，与后台的认证服务器进行通讯，如远程认证拨号用户服务器(RADIUS)交互。

解决可靠性、灵活性、可扩展性。



无线安全对策 – 封闭系统

封闭系统是指，一个对标为“Any”的SSID客户端不进行响应，并且不会向客户端详细地广播SSID的系统

当客户端在连接范围内搜索访问点时，封闭系统等待符合自身SSID的正确帧出现

优点

- 不会接受未识别网络的要求、比较容易实现

缺点

- 系统更新时，需重新发布服务区域认证ID、WEP密钥
- 设备更新带来的管理复杂度

无线安全对策 – 分配IP

利用LAN中的成熟技术保护WLAN

DHCP、静态IP

无线安全对策 - 无线安全防范 1

确保无线接入点放置在防火墙范围之外

MAC过滤

管理无线用户的ID

- 回避缺省SSID或网络名

WEP协议

- 回避缺省设置，经常更换密钥/口令

无线安全对策 - 无线安全防范 2

简化网络安全管理

- **不论用户是通过有线，还是无线方式进入网络，都采用集成化的单一用户ID和密码**

Radius - Remote Authentication Dial In User Service

- **采用VPN技术**

无线安全对策 - 扩展的移动安全体系结构 1

扩展的移动安全体系结构(EMSA)

- **无线设备层**
- **无线安全及漫游管理层**
- **数据库访问层**

无线安全对策 - 扩展的移动安全体系结构 2

无线设备层

- **无线设备层是核心功能层**
- **系统操作的对象**
  - **直接对象：AP设备**
  - **间接对象：由AP进行连接并通过AP设备进行网络访问的无线移动用户**
- **两个操作访问界面**
  - **AP设备访问层和Radius数据库访问层**

无线安全对策 - 扩展的移动安全体系结构 3

无线安全及漫游管理层

- **此层中包含了多个模块和模块引擎**
  - **无线设备发现引擎、无线设备组群管理引擎、无线设备维护模块**
  - **用户管理模块、移动用户漫游管理引擎**
  - **安全策略分析引擎、无线设备安全策略引擎**
  - **日志管理模块、预警模块**

无线安全对策 - 扩展的移动安全体系结构 4

数据库访问层

- **管理数据**
  - **实现无线安全和漫游管理**

常见攻击与弱点

无线安全对策

无线通信安全

无线VPN

蓝牙安全 1

蓝牙(Bluetooth)，Ericsson，1994

2.4GHz，ISM，GFSK调频

快跳频和短包技术

不同厂家设备在没有电线或者电缆情况下，近距离互操作归于统一

蓝牙安全 2

蓝牙安全模式

- **实体**
  - **蓝牙设备地址(BD_ADDR)：48bit的唯一地址**
  - **私人身份鉴定密钥：128bit**
  - **私人加密密钥：8bit～128bit**
  - **随机数(RAND)：128bit**

蓝牙安全 3

蓝牙安全三个模式

- **安全模式1(无安全)**
- **安全模式2(服务级加强安全)**
- **安全模式3(链路级加强安全)**

应用层安全加密

- **军事通信**

蓝牙安全体系结构 - 1

身份鉴定

授权

- **对信任设备的访问自动接受，而对不信任设备的访问必须经过授权**

Pairing/Bonding

- **用来产生连接双方的连接密钥**

加密

- **在接受服务之前，蓝牙设备的连接应该进入加密模式**

蓝牙安全体系结构 - 2

密钥管理

- **通过安全地管理密钥和分发密钥，禁止他人窃取**

应用灵活性

- **不同的服务可有不同的安全等级，在初始化后，使用者无须担心安全性，每项服务可以充当不同角色(客户/服务器)**

GSM安全 - 1

Global System for Mobile Communication

安全威胁

- **无线链路威胁**
- **服务网络威胁**
- **终端威胁**

GSM安全 - 2

安全威胁

- **无线链路威胁**
  - **攻击者窃听无线链路上的用户数据，甚至可以进行被动或主动的流量分析**
  - **修改或者删除无线链路上的合法用户的数据**
  - **在物理层或者协议层干扰用户数据的正确传输，来实现拒绝服务攻击**

GSM安全 - 3

安全威胁

- **服务网络威胁**
  - **攻击者在服务网内窃听用户数据，非授权访问在系统网络单元内的数据**
  - **修改或者删除用户数据，甚至假冒某一方修改数据**
  - **进行拒绝服务攻击**
  - **模拟合法用户使用网络服务，甚至假冒服务网以利用合法用户的接入尝试获得网络服务**

GSM安全 - 4

安全威胁

- **终端威胁**
  - **入侵者利用窃取的终端设备访问系统资源**
  - **利用终端设备访问系统中不允许访问的范围**
  - **修改或者删除终端的数据以破坏终端数据的完整性**

GSM安全 - 5

GSM安全机制

认证

- 通过对用户的鉴权来防止未授权用户的连接，这样保护用户不被假冒

加密

- 通过对传输过程进行加密可以防止信息在无线信道上被窃听，这样保护用户的隐私权

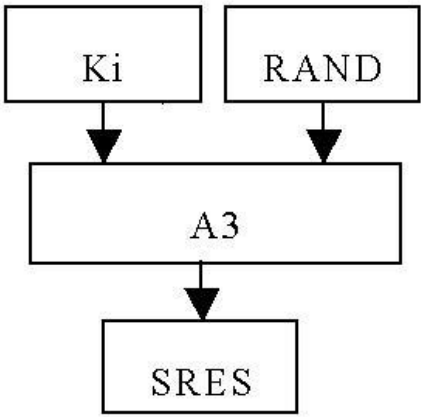
SIM卡

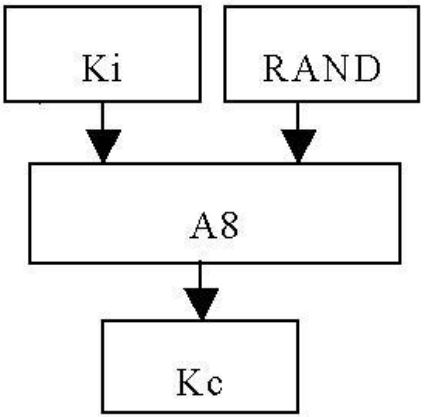
- 管理用户信息
- 临时号代替用户标识，防止追踪

GSM安全 - 6

认证机制

用户私钥　传回用户随机数



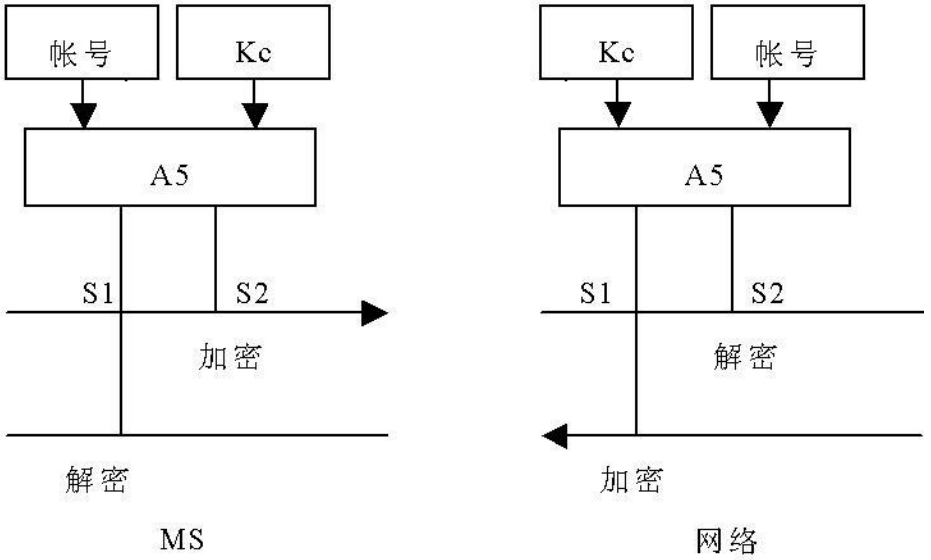


响应期望　　加密密钥

加密密钥，响应期望，随机数发送给服务中心，判断用户通过随机数计算的响应

GSM安全 - 7

加密机制



GSM安全 - 8

GSM的优点

- 结构简单
- 支持认证和加密
- 移动设备成本低、功耗低

GSM的缺点

- 加密和认证算法不足够强
- 敏感数据（密钥）在系统内部都采用明文进行传输
- 用户不可以改变认证密钥，这样无法避免重放攻击
- 没有消息完整性认证
- 只支持单向身份认证，无法防止伪造网络设备(例如基站)的恶意攻击
- 没有第三方仲裁功能（计费纠纷）
- 漫游时，服务网络采用的认证参数与归属网络之间没有有效的联系
- 缺乏升级能力

GPRS安全 - 1

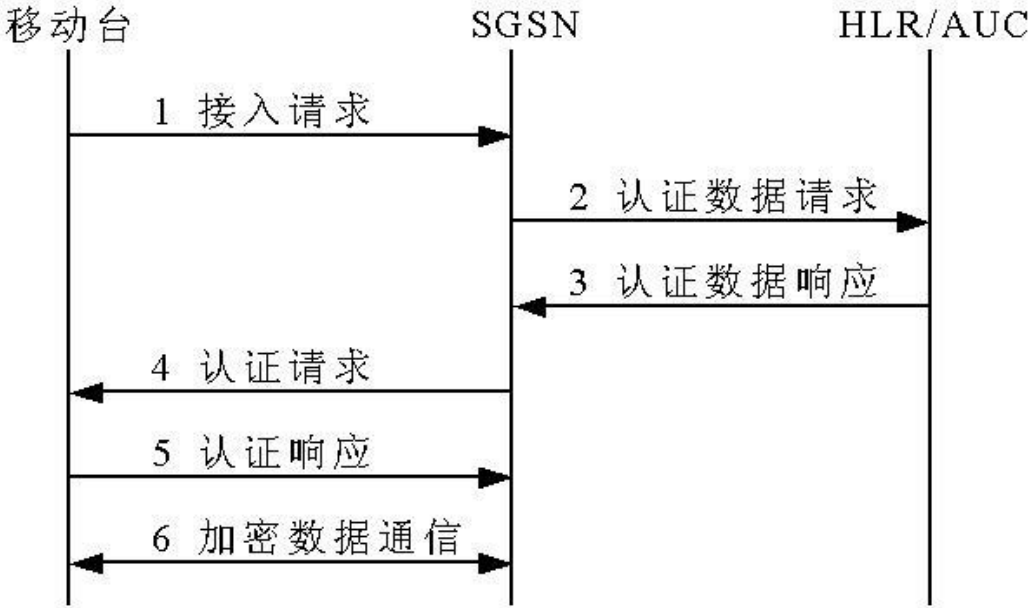
通用分组无线业务

GPRS可以在对现有的GSM网络改动并不大的情况下，通过增加一些网络节点来实现无线分组数据业务

在GSM安全的基础上加强了：身份保密、身份认证、用户数据保密、用户信令数据保密以及其他由GPRS系统提供的GSM标准之外的安全机制

GPRS安全 - 2

GPRS安全机制

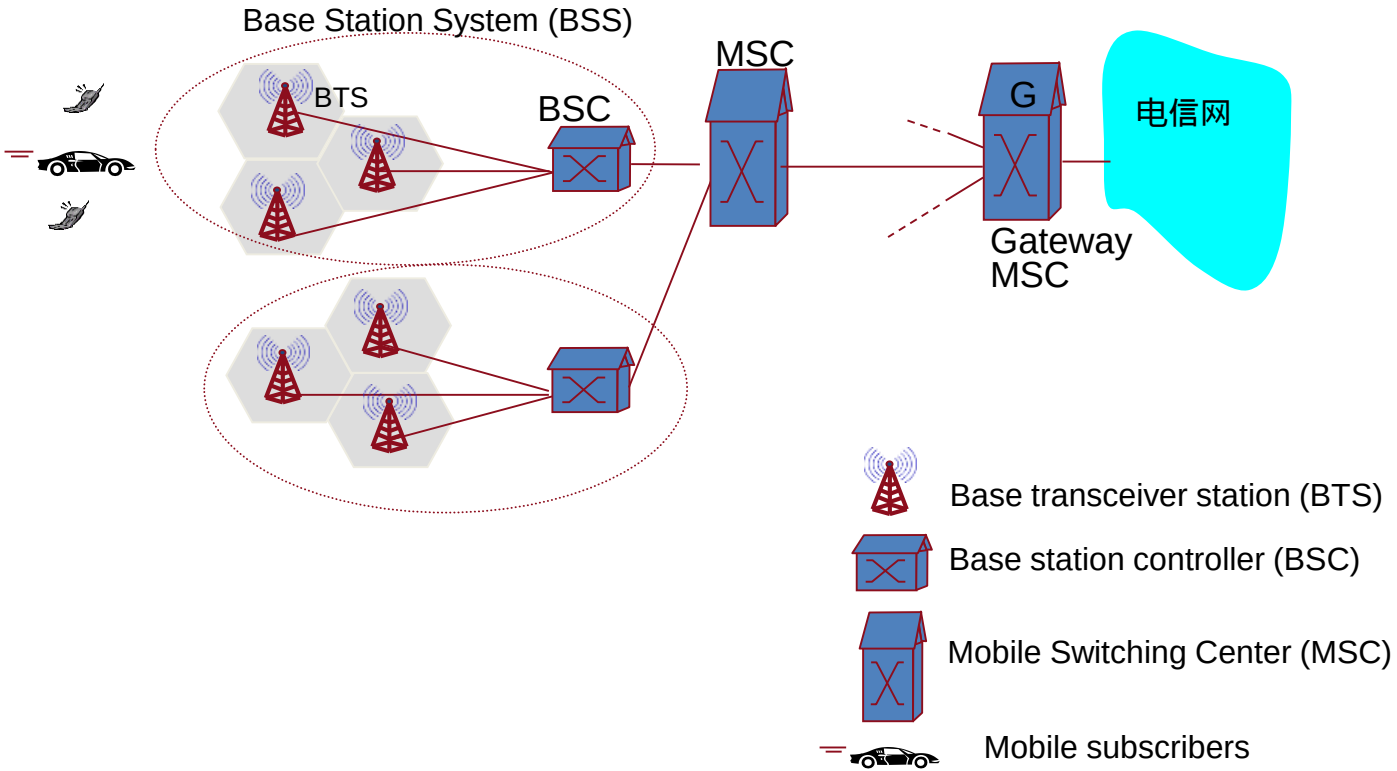


GPRS安全 - 3

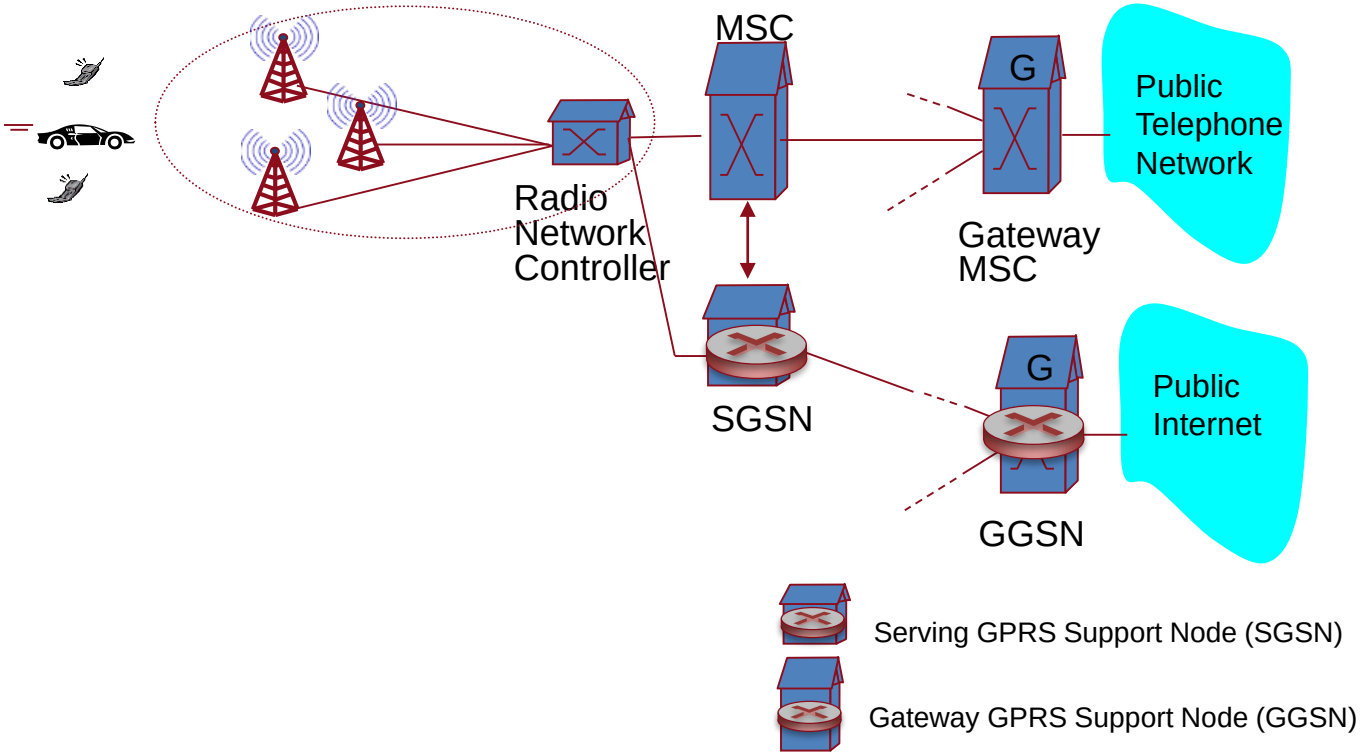
GPRS系统的安全缺陷

- **仍然是单向的（仅对用户认证）**
- **不提供端到端的加密（移动台与SGSN间会话过程）**
- **GEA算法的密钥长度太短(只有64位)**
- **SIM卡需要更好的安全保护**

GSM网络构架


Base Station System (BSS)
BTS
BSC
MSC
G
Gateway
MSC
电信网
Base transceiver station (BTS)
Base station controller (BSC)
Mobile Switching Center (MSC)
Mobile subscribers

3G网络构架


MSC
G
Public
Telephone
Network
Radio
Network
Controller
Gateway
MSC
SGSN
G
Public
Internet
GGSN
Serving GPRS Support Node (SGSN)
Gateway GPRS Support Node (GGSN)

3G安全 – 安全层次 1

网络接入安全：目的是抗击针对无线链路的攻击。

- 这其中主要包括身份保密、用户位置保密、用户行踪保密、实体身份认证、加密密钥分发、用户数据与信令数据的保密以及身份认证

核心网络安全：目的是保证核心网络实体之间能够安全地交换数据。

- 这其中包括网络实体间的身份认证、数据加密、消息认证以及对欺骗信息的收藏

3G安全 – 安全层次 2

用户安全：目的是保证对移动平台的安全接入。

- **这其中包括用户与智能卡之间的认证、智能卡与终端的认证以及其链路保护**

应用安全：目的是保证用户与服务提供商之间能够安全地交换应用程序的信息。

- **这其中包括应用实体间的身份认证、应用数据重放攻击的检测、应用数据完整性保护以及接入确定等**

3G安全 - 安全层次 3

安全特性可见性及可配置能力：

- **主要是指用户获知安全特性是否在使用，以及获知服务提供商的服务是否以安全服务为基础**

3G安全 – 安全特征

网络接入安全

网络安全

安全的可视性和可配置性

3G安全 - 网络接入安全

用户身份保密性(UIC)

- **此特征包括：用户身份保密性、用户位置保密性以及用户的不可追溯性**

实体认证

- **与实体认证相关的安全特征包括：认证协议、用户认证以及网络认证**

保密性

- **与数据保密性相关的安全特征包括：加密算法协议、加密密钥协议、用户数据的保密性和信令数据的保密性**

数据完整性

- **与网络接入链路上的数据完整性有关的安全特征包括：完整性算法协议、完整性密钥协议、数据完整性和信令数据的信源认证**

3G安全 - 安全特征

网络安全

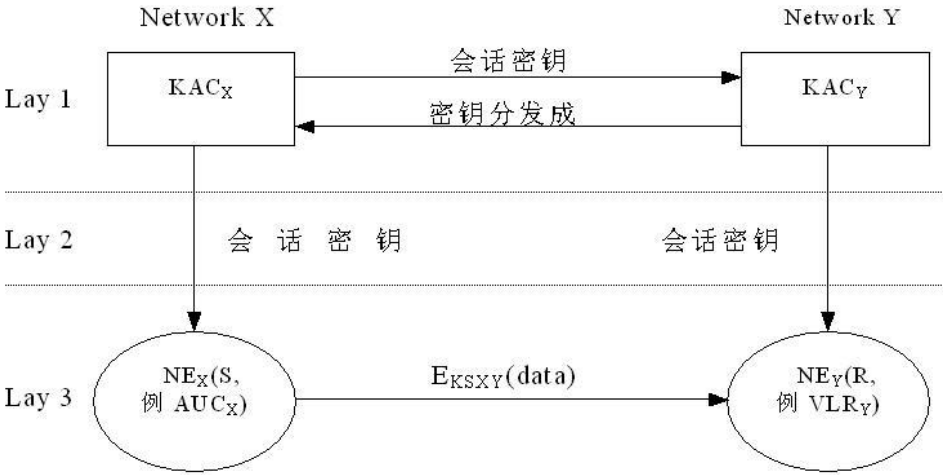
- 数据传输与应用

安全的可视性和可配置性

- 可视性
  - 接入网络的加密指示、安全等级指示等
- 可配置性
  - 用户USIM认证、非加密呼叫、非加密呼叫、某些加密算法的使用

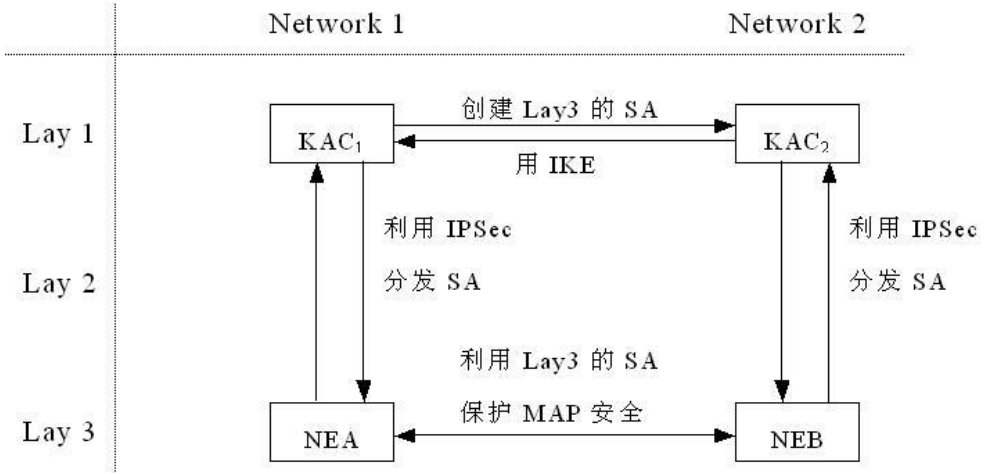
3G安全 – 密钥管理 1

不同网络实体间的密钥管理

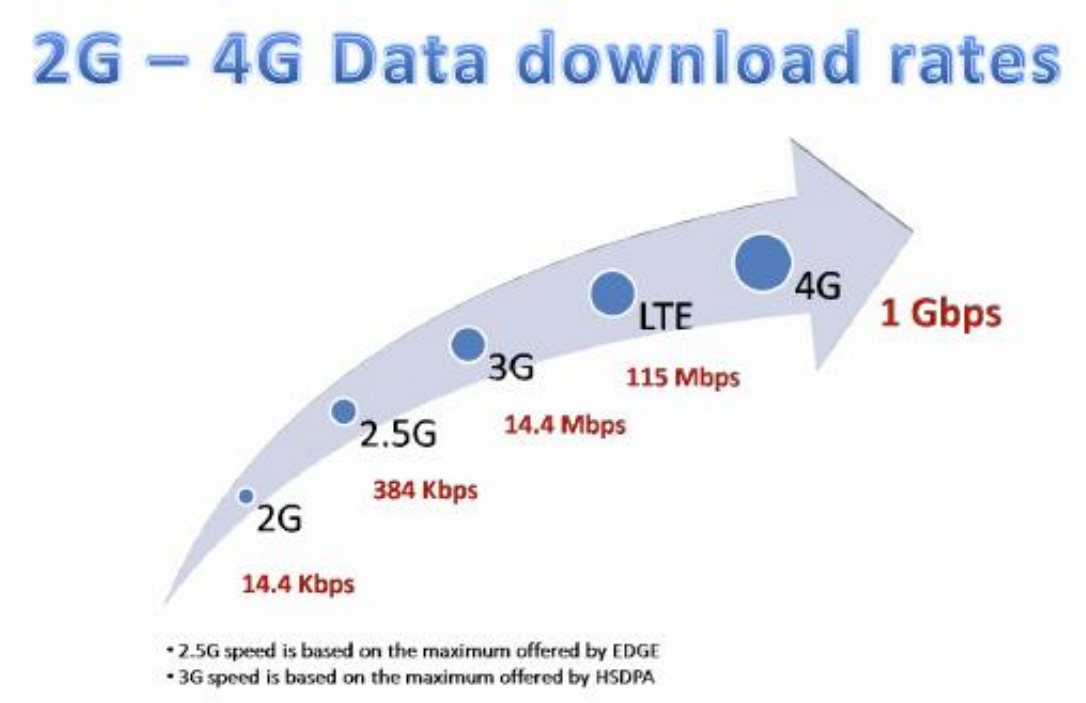


3G安全 - 密钥管理 2

两阶密钥管理结构



蜂窝网传输速度


2G – 4G Data download rates
2G
14.4 Kbps
2.5G
384 Kbps
3G
14.4 Mbps
LTE
115 Mbps
4G
1 Gbps
• 2.5G speed is based on the maximum offered by EDGE
• 3G speed is based on the maximum offered by HSDPA

常见攻击与弱点

无线安全对策

无线通信安全

无线VPN

无线VPN – 优势

简单性

多重密钥加密的传输（密钥更新）

不仅适用于个人用户，还适用于集团用户

无线VPN – 劣势

难以扩展（承载用户量）

技术复杂

价格昂贵（网关）

漫游功能有限（由终端设备决定）

没有管理控制（隧道流量）

课后习题

1. 如何判断自己的WLAN是安全的?

2. 要实现彻底的无线网络安全情况，需要的最小功能是什么?

3. 与GSM系统、GPRS系统相比，3G系统的安全保护的特殊性在哪里?

无线安全对策 - 无线安全防范 1

确保无线接入点放置在防火墙范围之外

MAC过滤

管理无线用户的ID

- 回避缺省SSID或网络名

WEP协议

- 回避缺省设置，经常更换密钥/口令

无线安全对策 - 无线安全防范 2

简化网络安全管理

- **不论用户是通过有线，还是无线方式进入网络，都采用集成化的单一用户ID和密码**

Radius - Remote Authentication Dial In User Service

- **采用VPN技术**

谢谢!