通 信 安 全

L13—通信安全新挑战

- 教师：崔爱娇

- 编号：ELEC3019
- 学时：32学时

概 要

通信安全新挑战

- 电话网攻击
- 手机病毒
- SIM卡攻击
- 移动多媒体版权保护

概 要

通信安全新挑战

- 电话网攻击
- 手机病毒
- SIM卡攻击
- 移动多媒体版权保护

电话网安全问题

随着信息技术的飞速发展和广泛应用，电话网络的安全问题已经成了直接关系到国家安全和经济安全的大问题。近年来，危害电话网的行为时有发生。

电话网发展历史上的安全事件

在电话网出现的同时，电话网安全问题也就随之而生。如盗打电话、破坏通信链路、篡改计费信息等

目前最为突出的电话网攻击就是盗打电话，在Internet上，可以搜到数千页有关盗打电话的网页。甚至还有些盗打电话程序和黑客软件一样，出现在黑客网站里，可以随意下载执行

电话网安全问题

电话网的开放化和数字化趋势

电话网已不再是原来的封闭、独立的网络。随着电话网尤其是其支撑信令网的开放，电话网的运行将不完全在运营商的控制之下。

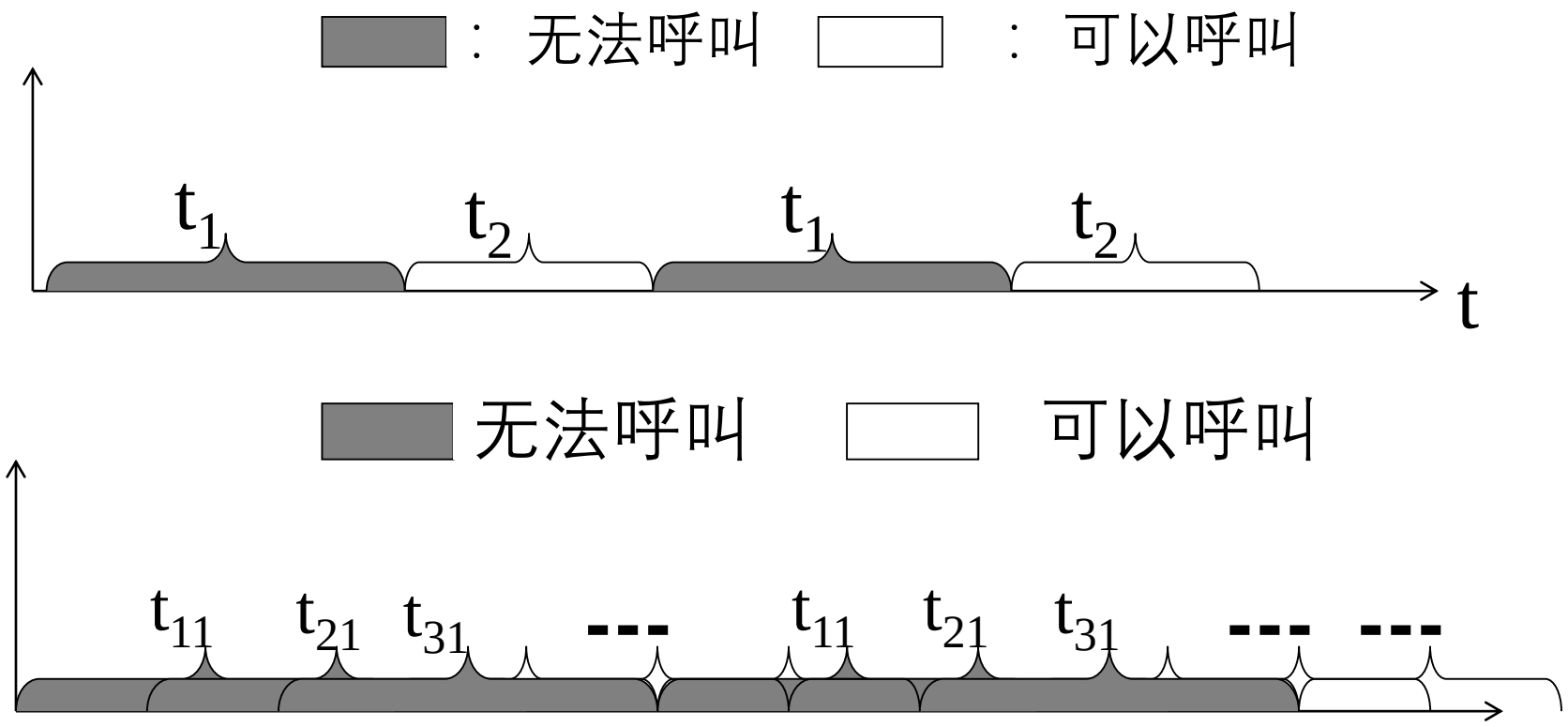
电话网攻击的分类

- 针对用户终端设备的攻击
- 针对交换设备的攻击
- 针对电信数据库的攻击
- 针对网管系统的攻击
- 针对信令系统的攻击
- 针对传输设备的攻击

拒绝服务攻击

用户终端拒绝服务攻击

所谓电话网用户终端拒绝服务攻击是指攻击者使用专用的拨号硬件或软件，对攻击对象发起的拨号攻击。



电话终端拒绝服务攻击示意图

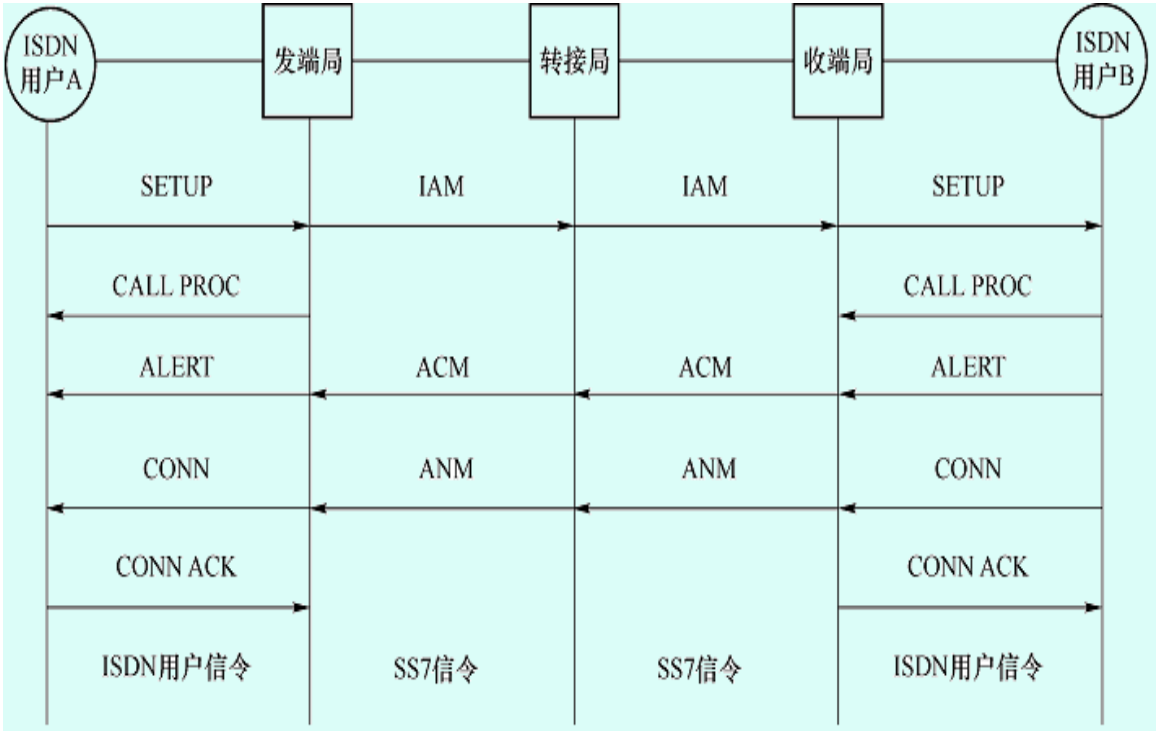
拒绝服务攻击

这种攻击方式可以对单一目标号码进行攻击，也可以对一组号码进行攻击（群发攻击）。

这种攻击方式借鉴自Internet上的SYN flood攻击。SYN flood利用了TCP三步握手容易导致拒绝服务攻击的漏洞

交换设备拒绝服务攻击

拒绝服务攻击用于用户终端时，受到影响的只是个别用户，而同样的攻击方式如果用于交换设备则该设备所属的所有用户都无法使用正常的电话服务。如果网络中的骨干交换机受到拒绝服务攻击，所有通过的话务都要受到影响。



ISDN呼叫建立示意图

账户口令窃取

攻击方式与原理：普通的电话网应用平台的账户/密码的传递方式都是以DTMF方式直接在电话线上明文传输。搭线窃听，并通过简单的DTMF解码器就可以读取电话线上传输的账号和密码

在更高级的攻击中，甚至连物理上的搭线都不需要，因为电话线周围存在电磁泄漏，使用专用的电磁接受设备在离电话线一定距离之内就可以获取线路上的信息。

解决方案：据统计，系统被非法进入60%是从攻破密码开始的

账户口令窃取

低群/Hz	高群/Hz			
	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

双音多频 DTMF（Dual Tone Multi Frequency），双音多频，由高频群和低频群组成，高低频群各包含4个频率。一个高频信号和一个低频信号叠加组成一个组合信号，代表一个数字。DTMF信号有16个编码。利用DTMF信令可选择呼叫相应的对讲机。

针对信令网的攻击

- 敏感信息窃听攻击
- 对信令点SP的DoS攻击
- 对信令转接点STP的DoS攻击
- 其他窃听、篡改、拦截、干扰攻击
- 针对协议实现的攻击
- 各种组合攻击

概 要

通信安全新挑战

- 电话网攻击
- 手机病毒
- SIM卡攻击
- 移动多媒体版权保护

手机病毒

业务的开放性，在为移动业务增添活力的同时，也为利用手机传播病毒、在手机中植入木马、破坏手机功能、盗用手机内部信息提供了可能。

这里所说的手机病毒，指的是对手机系统产生破坏、控制或给终端用户造成损失或不便的程序，熟知的PC病毒的定义更广。

短信类手机病毒

短信类手机病毒主要是利用手机操作系统本身的一种缺陷—BUG而编写的一种进行恶意攻击或者操作的代码，病毒是诱因，但Bug为病毒的攻击提供了机会和渠道

工作原理是：手机对于收到的信息（包括短信、彩信、铃声、图片等），首先要经过手机操作系统对其进行翻译，然后才能使用或查看，而目前的恶意短信攻击就是利用了这一点，编制出针对某种操作系统的漏洞的短消息内容，攻击手机

短信类手机病毒

1、利用手机对SMS协议处理漏洞

2、利用手机对某些特殊字符的处理漏洞

3、利用手机操作系统应用软件的漏洞

手机病毒

炸弹类手机病毒

该类病毒就是利用短信网站或者利用网关漏洞向手机发送大量短信，进行短信拒绝服务攻击。

蠕虫类手机病毒

目前出现的蠕虫病毒是利用蓝牙手机的一个缺陷而进行传播的，这是手机厂商在实现蓝牙标准的方式引起的

手机病毒

木马类手机病毒

目前出现了一种针对Symbian操作系统的木马“Mosquitoes Trojan”，Mosquitoes是一款游戏的名称，程序编写者在游戏中植入了向某一目的地发送短消息的代码，当用户启动该程序时，它就会定时向一些高收费的短信地址发送短信，从而给用户造成经济上的损失

手机病毒

以上的手机病毒还不具有很大的危害性

a. 智能手机的出现还是近一两年的事，人们对该操作系统熟悉程度还不够。

b. 手机所采用的芯片也是专用的，平时很难接触到。

c. 手机系统中可以“写”的地方太少。

d. 手机中核心程序都是固化在ROM中的，对于第三方只有读的权限或者连这种权限都没有。

真正具有破坏性的病毒还有一段时间，但一旦发现，其危害程度将远远超过网络病毒，这只是一个时间的问题

概 要

通信安全新挑战

- 电话网攻击
- 手机病毒
- SIM卡攻击
- 移动多媒体版权保护

SIM卡攻击

从对用户的影响角度分析，攻击者对于SIM卡的攻击行为主要是为了实现两个目的：影响用户正常使用网络服务，或者通过获取SIM卡的密钥KI来获得经济利益

SIM卡攻击

针对手机漏洞的短消息攻击

利用这种方式对手机发起攻击的手段主要有：

a. Nokia某些产品PDU格式漏洞

b. 西门子的"%String"漏洞

c. Nokia的Vcard漏洞

d. 切断攻击短消息的传播途径

e. 手机防御体系

SIM卡攻击

针对SIM卡短消息协议处理漏洞的攻击

防御措施：最重要的是增强SIM卡操作系统COS的健壮性，在处理短消息协议时，充分考虑到各种异常情况，保证在出现这些异常情况时，不影响SIM卡的正常使用

SIM卡攻击

利用短消息网站漏洞的拒绝服务攻击

攻击者利用短消息网站的短消息服务功能向目标用户发送大量短消息，影响目标用户正常使用网络功能的拒绝服务攻击就成为一种攻击手段

这种攻击手段具有比较明显的特征，即在短时间内通过网站向特定的手机发送大量短消息，因此，应该从短消息的源头和目的地两方面入手制定相应的措施

SIM卡攻击

直接拒绝服务攻击

如果攻击者并不特别在意攻击的成本，那么可以利用直接拒绝服务方式攻击他人，即利用快速的专用发送设备（内置SIM卡）向同一个用户发送大量的短消息，影响用户使用网络功能和SIM卡的使用寿命

通过专用发送设备如无线调制解调器还可以编辑和发送二级短消息，这种短消息到达用户手机时，并不向用户发出相应的提示信息，从而更具有欺骗性，更加令人防不胜防

SIM卡旁路攻击

- 通过对这些旁路信息进行分析，从而获得有关算法和密钥信息的攻击手段就被称为旁路攻击。
- 电源分析攻击就是一种旁路攻击方式

SIM卡旁路攻击

伪装手机实施SIM卡攻击

SIM卡并没有能力识别自己是不是在与手机通信，所以攻击者可以利用标准的读卡器来伪装手机，将SIM卡插入读卡器中，向SIM卡发送SELECT指令从而获取IMSI

同样，攻击者也可以利用读卡器伪装手机，将RAND发送给SIM卡，并发送RUN GSM ALGORITHM 指令（该指令的执行条件同样是PIN码），要求SIM卡运行COMP128算法并返回SRES和Kc，然后对SRES和Kc进行分析以破解KI

SIM卡旁路攻击

伪装基站实施SIM卡攻击

通过伪装基站的方式实施SIM卡攻击的原理同样是利用了GSM系统单向认证的安全缺陷，即网络可以认证用户SIM卡的身份，而用户SIM卡无法鉴别网络的身份。此外，COMP128算法存在碰撞现象的漏洞也是这种攻击方式所要利用的主要手段

破解KI的流程与上小节中描述的流程基本一致，不同之处在于此时攻击者与用户SIM卡之间的数据接口不再是读卡器和I/O接口，而是空中的无线接口了

由于手机必须响应伪基站的每一个鉴权挑战RAND，所以攻击者可以不断地给目标手机发送鉴权挑战，由手机将RAND传送给SIM卡，发送鉴权指令，并将鉴权响应返回给伪基站

在整个攻击过程中，攻击者设置的伪基站必须能够一直访问目标手机，一旦在破解出全部KI之前，用户离开了伪基站的控制区域，攻击者的努力将半途而废。不过，由于通过伪基站的方式可以同时访问更多的手机，其危害也大于伪装手机的方式

概 要

通信安全新挑战

- 电话网攻击
- 手机病毒
- SIM卡攻击
- 移动多媒体版权保护

移动多媒体版权保护

数字水印技术的应用，不仅可以达到版权控制的目的，而且还在一定程度上阻止了不良用户对版权的破坏，弥补了加密等方式的不足

数字水印版权管理系统原理

WDRM系统的中心为DRMC（数字版权管理中心），负责对数字内容版权的封装、检测、管理

DRMC内部分为版权注册、版权检测和版权管理**三个功能模块**，由版权注册装置、版权管理装置、版权控制装置、版权计费装置、版权跟踪装置和数字内容门户**六部分**组成，需要保存（SPISDN、TZM(M')）数据库，并可选保存（TZM（M'），MSISDN，发送权限，接收权限）数据库。

移动多媒体版权保护

1 数字内容版权的注册封装

1)SP将需要注册版权的数字内容M发送到DRMC的注册功能模块；

2)DRMC对数字内容M尝试提取水印，判断是否已经加过版权水印，若加过，则通知SP，并退出注册过程；

3)DRMC的注册模块针对数字内容M生成注册信息S＝（CPISDN、SPISDN、注册标记、其他版权信息等），即版权水印；

4)将S使用密钥Key，采用数字水印方案嵌入到M中，得到M’；

5)DRMC获取M’的特征TZM（M’）；

6)记录SPISDN、TZM(M’)，并保证数据库中项目唯一；

7) DRM将M’通过专用通道发送回给SP，完成版权注册。

移动多媒体版权保护

数字内容的下载

WDRM的DRMC接收来自MMSC的版权检测请求或直接获得数字内容，并根据用户的权限和数字内容的约束进行相应的处理

数字内容的正常转发

目前，用户终端在接收到数字内容后，可以将其任意转发，而不收取版权使用费。通过对数字内容添加版权水印，DRMC在转发数字内容时就可以判断数字内容的版权所有，从而正确收取版权使用费。

移动多媒体版权保护

数字内容破坏后的转发

假设用户A拥有以下对版权的破坏能力：

- 用户A有能力对已经注册版权的数字内容进行修改；
- 用户A可以获得其接收到的数据流，从而从数据结构上进行破坏版权的处理，如直接去除嵌名。

移动多媒体版权保护

此外，数字内容在传输过程中，MMSC等设备也可能对数字内容进行改动，导致非故意的破坏。因此，当数字内容被转发时，DRMC得到的数字内容可能就不完整，可能的形式有：

- 只有数字内容M’
- 数字内容被破坏M”+EM’
- 数字内容和签名均被破坏M”

移动多媒体版权保护

- **针对这些形式，DRMC的处理流程如下：**

➢DRMC接收到被破坏后的数字内容，可能是上述三种形式之一，判断是否含有签名信息，即EM’；

➢若含有EM’，则数字内容为M”＋EM’，此时拒绝转发；

移动多媒体版权保护

WDRM的实时性考虑

综上所述，可以看出当数字内容到达DRMC后，可能经历的处理有加解密、提取特征、查表和提取水印操作。而且，只有当签名和数字内容不一致时才经历提取水印的操作。

此外，在实际实施时，也可以记录直接提取水印和查表方式的处理时间，实时选择时效高的操作或直接采用两种方式并行处理来获取版权

移动多媒体版权保护

WDRM安全性分析

从管理角度来说，WDRM的安全性取决于水印算法安全性和密钥安全性。**水印算法的安全性**是指水印算法应是保密的、不公开的，同时其安全性也指嵌入的水印满足水印的一般特性。

密钥分配和管理

为了提高水印的安全性，在加载水印时可以用密钥进行加载，这就涉及到密钥分配和管理问题。

算法管理

注册水印我们采取双层水印技术，其中第二层水印包含的信息有密钥编号、算法编号和注册标识，这些信息不需要保密，所以使用的算法也不需要更新。需要更新的是第一层水印所使用的水印算法