INDEX

@加密之王Enigma

@计算机网络安全风险

@计算机网络安全体系结构

加密之王Enigma

Enigma：二战中最大的军事秘密

@1939年爆发第二次世界大战，历时6年，60多个国家和地区参战，波及20多亿人口，战争交战各方共动员军队1亿多人

@二战中最大的军事秘密，除了原子弹外，就是纳粹德国的核心加密机——Enigma

@在这场人类有史以来最惨烈的战争中，决定最后战争命运走向的竟然是几台机器和制造它们的天才数学家们

Enigma的工作原理

@Enigma是一种转轮式密码机，原理并不复杂，但在第二次世界大战之前要破解它却基本上是不可能的

@从外表看起来， Enigma似乎跟普通的打字机别无二致，通常有三个部分组成：键盘、转轮和显示器

@为了让密电尽量简短和难以破译，Enigma的键盘没有空格和标点符号

@Enigma使用的加密方法叫做代换密码算法（Substitution cipher）

转轮机

@为了防止字频统计，阿瑟发明了Enigma最关键的加密部件——转轮机（Rotor machine）

@转轮机是会自动转动替换对应字母的设备，单表代换密码变成多表代换密码，强度大大增加

@当在Enigma键盘上一个键被按下时，相应的密文在显示器上显示，转轮的方向就自动地转动一个字母的位置

@例如，当第一次键入a时，信号通过转轮中的连线，灯D亮起来，放开键后，转轮转动一格，各字母所对应的密码就改变了；第二次键入a时，它所对应的字母就变成了H；转轮又转动一格，第三次键入a时，灯K亮起来

反射器

@在此基础上，阿瑟更是十分巧妙地在三个转轮的一端加上了一个反射器

@Enigma把键盘和显示器中的相同字母用电线连在一起；反射器和转轮一样，把某一个字母连在另一个字母上，但是它并不转动

@事实上它只是一个巧妙的开关：当一个键被按下时，通过三个转轮连成的一条线路，然后经过反射器再回到三个转轮，通过另一条线路再到达显示器上

@反射器虽然没有像转轮那样增加可能的不重复的方向，但是它可以使译码的过程和编码的过程完全一样，大大的提高了使用的简洁性

Enigma的工作过程

@开启一台Enigma，首先调节Enigma三个转轮方向，使它们出于初始方向

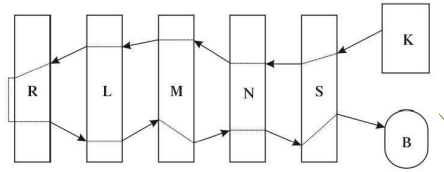
@转轮的初始方向就密匙，这是收发双方事前就预先约定好的秘密

@按照明文敲打键盘，在Enigma的显示器中，每个被键入的字母的密文都依次闪亮并被记录下来，接着它把密文通过电报传送出去

@接收在接收到密文电报后，打开同样的Enigma，调节好三个转轮的初始方向，通过键盘键入密文，明文就依次显示在屏幕上，并被记录下来

Enigma密码机加密原理

Enigma M3型密码编码路径图



- N 、L、M为3个不同的滚轮
- R为反射器
- S为接线板
- K为键盘
- B为灯板

Enigma：滚轮和反射器的设置

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
N1	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O	B
N2	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O	B	D

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T

Enigma举例

@假设滚轮的顺序为N、L、M，而三个滚轮的初始位置为AAA，接线板上不用任何接线。试求输入明文为“AA”，则密文为“DH”。

@从键盘K按下第一个明文字母“A”，由于接线板无接线，字母“A”保持不变

@按键使得滚轮N向前滚动一格(即N1)，滚轮M和L皆保持不变

@如果解密“DH”呢？

滚轮	字母
N	A→D
M	D→K
L	K→N
R	N→K
L	K→B
M	B→J
N	J→D

滚轮	字母
N	A→F
M	F→I
L	I→V
R	V→W
L	W→N
M	N→T
N	T→H

增加强度

@三个转轮的初始方向共有26*26*26=17576个选择，可以进行蛮力破译

@增加转轮个数：体积过大，易用性差

@阿瑟提出了两个更巧妙的改进

@把Enigma的三个加密转轮制作成为可方便自由拆卸的形式，用户可以自行调整顺序

@在Enigma的键盘和第一个转轮之间增加了一个连接板，连接板能够让使用者用一根信号线将某一个字母和另外一个字母任意连接，这样这个字母的信号在进入转轮之前就会转变为另一个字母的信号。这种连线最多可以有六根甚至更多

增加强度

@当然，转轮自身的初始方向，转轮之间的相互位置，以及连接板连线的状况都需要双方事先商定好，并严格保密

@这样改动的Enigma一共到底有多少种组合加密可能性呢？

@三个转轮不同的方向组成了26*26*26=17576种

@三个转轮间不同的相对位置为6种

@连接板上两两交换6对字母的可能性数目非常巨大，有100391791500种；

@于是一共有17576*6*100391791500，大约为一亿亿种可能性

加密之王

@强大的Enigma让德国军方的加密信心显得无比十足

@造价却低廉的Enigma却具有如此强悍的加密方式，盟军第一次开始品尝到加密的噩梦

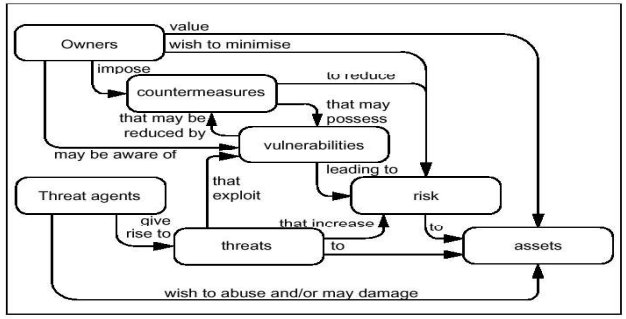
@Enigma成为了战争史上最成功的信息加密之王

计算机网络安全风险

风险分析模型

@资产(Asset) 脆弱性(Vulnerability) 威胁(Threat) 风险(risk)

@防范 (Countermeasure) 预防(Prevention)/检测(detection)/响应(response)



资产 Asset

@资产： 安全保护的对象

@资产的定义

- @组织业务开展必需的、被安全措施所保护的信息、信息处理系统、信息传输系统等资源

@资产的举例

- @计算机系统：硬件、软件、外设
- @网络基础设施：路由器、交换机、拓扑结构信息、带宽
- @业务数据：信息、计算机软件

@资产价值（Asset Value）

- @信息本身的价值
- @支持软件及维护的价值
- @丧失保密性、完整性、可用性的损失

威胁 Threat

@系统故障

- @电源故障
- @硬件故障
- @软件故障

@自然灾害和战争的威胁

- @风雨雷电、地震、火灾
- @战争等

@人为的威胁

- @误操作
- @泄密、窃密、篡改数据
- @盗用资源
  (计算资源, 通信资源, 存储资源)
- @拒绝服务
  (主机, 网络设备 , 通信带宽)
- @病毒、蠕虫等恶意代码

防范 Countermeasure

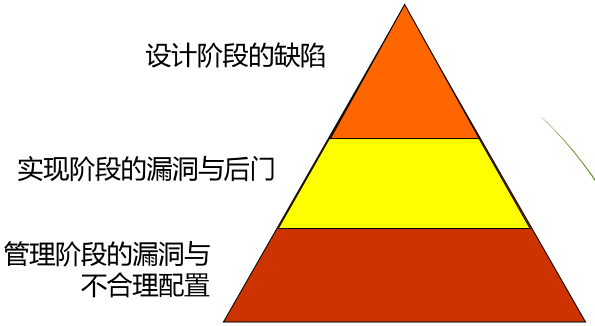
	预防	检测	恢复
管理	政策、程序、培训	审计制度	应急计划
技术	认证系统 防火墙等	入侵检测系统	数据备份 自动恢复系统
物理	防盗门 物理隔离	录像 监控措施	设备备份 线路备份等

脆弱性 Vulnerabilities

@Vulnerabilities： 脆弱性，弱点，缺陷，漏洞

@脆弱性主要来自于两个方面
- @计算机网络自身的脆弱性
  - @设计阶段的漏洞
  - @实现阶段的漏洞与后门
  - @管理阶段的漏洞与不合理配置
- @安全管理制度的脆弱性

计算机网络自身的脆弱性



设计阶段的脆弱性

@在Internet的设计阶段，Internet首先应用于研究环境，可信的、少量的用户群体。基本不考虑安全问题

@在早期的RFC中明确说明：
“Security issues are not discussed in this memo.”

@所设计的多数协议没有提供安全机制：
- @缺乏安全的认证机制，比如SMTP, telnet
- @明码传输，不提供保密性服务
- @没有服务质量(QoS)保证

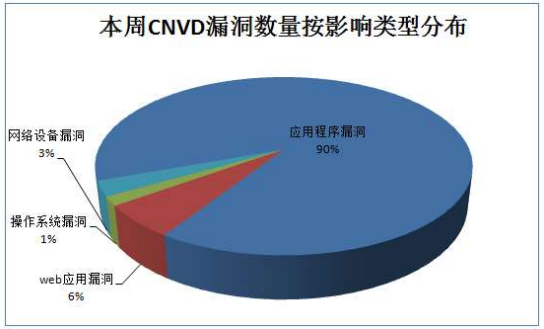
实现阶段和配置维护阶段的脆弱性

@实现阶段
- @软件越来越复杂、庞大，市场竞争导致很多代码没有经过严格的质量控制
- @无意的软件漏洞，如 buffer overflow
- @有意的后门

@配置维护阶段
- @系统的缺省安装
- @弱口令等

触目惊心的漏洞们

@http://www.cnvd.org.cn/ @http://www.sans.org/



安全管理制度的脆弱性

@网络和系统管理工作变得越来越困难
- @安全政策不明确：目标不明、责任不清、惩罚不力
- @动态变化的环境：业务发展，人员流动

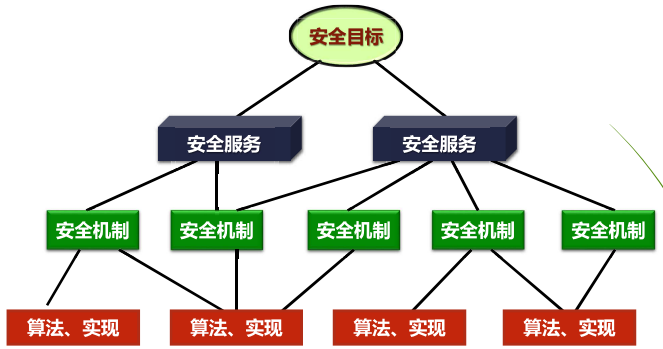
@社会问题
- @道德问题
- @法律问题：立法问题、执法问题

@国际间的协作问题
- @政治、文化、法律等障碍

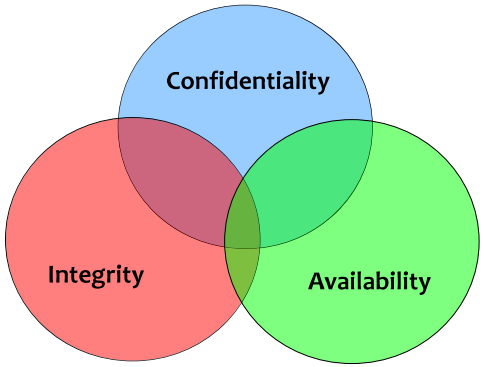
计算机网络安全体系结构

安全目标CIA / 安全服务 / 安全机制

安全目标、服务、机制的关系



安全目标： CIA



安全目标 ： CIA

@Confidentiality：保密性、机密性

- @保护信息内容不会被泄露给未授权的实体
- @业务数据、网络拓扑、流量都可能有保密性要求
- @防止被动攻击

@Integrity：完整性

- @保证信息不被未授权地修改，或者如果被修改可以检测出来
- @防止主动攻击，比如篡改、插入、重放

安全目标：CIA

@Availability：可用性

- @保证资源的授权用户能够访问到应得资源或服务，防止拒绝服务攻击
- @对计算机系统可用性的攻击
- @路由交换设备的处理能力、缓冲区
- @链路带宽

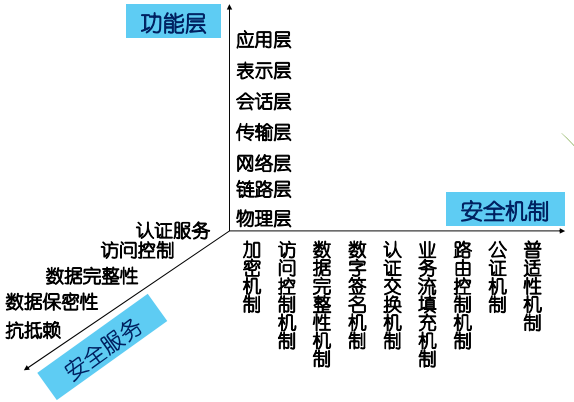
OSI安全框架

@ITU-T推荐方案X.800，即OSI安全框架，定义了一种系统方法，为网络管理员提供了一种安全的组织方法

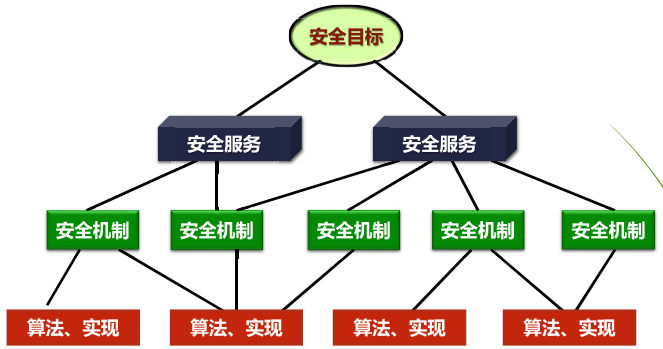
@OSI安全框架主要关注安全服务、安全机制和安全攻击

- @安全服务：
  一种由系统提供的对系统自愿进行特殊的处理或通信服务，安全服务通过安全机制来实现安全策略。(RFC 2828)
- @安全机制：
  用来保护系统免受监听、阻止安全攻击及恢复系统的机制
- @安全攻击：
  主动攻击、被动攻击。

OSI安全体系结构



安全目标、服务、机制的关系



安全服务

@X.800提供了下面一些的安全服务：

- @Authentication：认证服务
- @Confidentiality：保密服务
- @Integrity：数据完整性保护
- @Access Control：访问控制服务
- @Non-repudiation：抗抵赖服务
- @Availability：可用性服务

认证服务 Authentication

@认证服务与保证通信的真实性有关

@在单条消息的情况下：

- @认证服务向接受方保证发送方的真实性

@在双方通信的时候：

- @在连接的初始化阶段，认证服务保证双方的真实性
- @认证服务还需要保证该连接不受第三方非法干扰：第三方能够伪装成两个实体中一个进行非授权的传输或者接收数据

认证服务 Authentication

@两个特殊的认证服务：

- @对等实体认证（Peer Authentication）
  - @参与通信的实体的身份是真实的
  - @一个实体不能试图进行伪装或者对以前连接进行非授权的重放
  - @面向连接的应用
- @数据源认证（Data original authentication）
  - @对数据的来源提供确认，但是对数据的复制和修改不提供保护
  - @保证接收到的信息的确来自它所宣称的来源
  - @面向无连接的应用

保密服务 Confidentiality

@保密性是防止传输的数据遭到被动攻击

- @连接保密服务与无连接保密服务
- @保密力度
  - @流(stream)、消息(message)、选择字段(field)

@保密性的另一方面是防止流量分析

- @防止攻击者观察到消息的源、目的、频率、长度或者其它流量特征

数据完整性服务 Integrity

@完整性可对消息流、单条消息或者消息的选定部分的进行保护

@面向连接的完整性服务保证收到的消息和发出的消息一致

@面向无连接的完整性服务仅保证单条消息不被修改

@完整性服务与主动攻击有关，我们更关心的是检测而不是阻止攻击

访问控制服务Access Control

@限制实体的访问权限，通常是经过认证的合法的实体才可以访问

@标识与认证是访问控制的前提

抗抵赖服务 Non-repudiation

@抗抵赖服务防止发送方或者接收方否认传输或者接收过某条消息

@源发抗抵赖

@消息发出后，接收方能够证明消息是由声称的发送方发出的

@交付抗抵赖

@消息接收后，发送方能够证明消息事实上确实由声称的接收方收到了

可用性服务 Availability

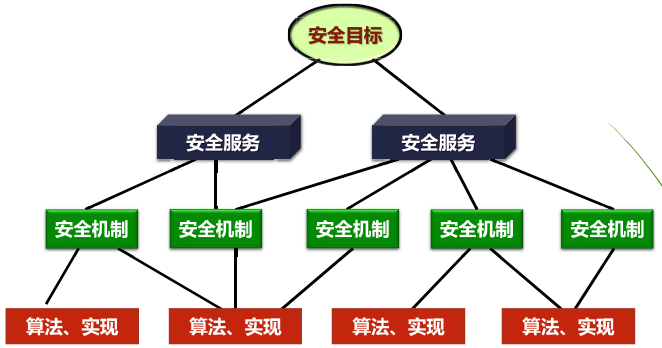
@可用性的定义

@根据系统的性能说明，能够按照授权的系统实体的要求存取或使用系统或系统资源的性质。

@资源冗余（备份）

@灾难恢复

安全目标、服务、机制的关系



安全机制

@安全机制分成两类：

@特定安全机制
在特定的协议层实现的安全机制

@普通的安全机制
不属于任何协议层或者安全服务的安全机制

普通的安全机制

- 可信功能(trusted functions)
  - 根据某些标准被认为是正确的
- 安全标签(security Labels)
  - 资源的标志，指明该资源的安全属性
- 事件检测 (Event Detection)
  - 检测与安全相关的事件
- 审计跟踪 (security audit Trail)
  - 收集潜在用于安全审计的数据，对系统记录和行为的独立回顾和检查
- 安全恢复 (security recovery)
  - 处理来自安全机制的请求，如事件处理、管理功能和采取恢复行为

特定安全机制(1)

- 加密机制（密码机制）
  - 运用数学算法将数据转换成不可知的形式
  - 数据的变换和复原依赖于算法和零个或者多个加密密钥
  - 算法可以是可逆的，也可以是不可逆的
  - 可以支持数据保密性、完整性等多种安全服务
- 数字签名机制
  - 附加于数据元之后的数据，是对数据元的密码变换，以使得（如接收方）可以证明数据源和完整性，并防止伪造
  - 签名：使用签名者独有的私有信息
  - 验证：使用公开的信息和规程

特定安全机制(2)

- 访问控制机制
  - 对资源进行访问控制的各种机制
  - 实体必须经过认证，可用在源点/中间/目的
  - 访问控制可以基于以下手段：
    - 集中的授权信息库
    - 主体的能力表
    - 客体的访问控制链表
    - 主体和客体的安全标签或安全级别
    - 路由、时间、位置等

特定安全机制(3)

- 数据完整性机制
  - 用于保证数据元或者数据元流的完整性的各种机制
  - 数据元序列
    - 序列号
    - 时间戳
- 通信业务流量填充机制
  - 在数据流空隙中插入若干位以阻止流量分析

特定安全机制(4)

- 认证交换机制
  - 通过信息交换来保证实体身份的各种机制
  - 用于认证交换的技术包括：
    - 认证信息，如口令
    - 密码技术
    - 被认证实体的特征
  - 为防止重放攻击，认证交换机制常与以下技术结合使用：
    - 时间戳、两次或三次握手、数字签名

特定安全机制(5)

- 路由控制机制
  - 路由能动态地或预定地选取，以便只使用物理上安全的子网、中继站或链路
  - 在检测到持续的操作攻击时，端系统希望指示网络服务的提供者经不同的路由建立连接
  - 带有某些安全标记的数据可能被安全策略禁止通过某些子网、中继或链路。连接的发起者(或无连接数据单元的发送者)可以指定路由选择说明，由它请求回避某些特定的子网络、链路或中继

特定安全机制(6)

@公证机制

- @利用可信任的第三方来保证数据交换的某些性质
- @这种保证是由第三方公证人提供的。公证人为通信实体所信任，并掌握必要信息以一种可证实方式提供所需的保证
- @有关在两个或多个实体之间通信的数据的性质，如它的完整性、原发、时间和目的地等能够借助公证机制而得到确保
- @每个通信事例可使用数字签名、加密和完整性机制以适应公证人提供的那种服务。当这种公证机制被用到时，数据便在参与通信的实体之间经由受保护的通信实例和公证方进行通信

安全性攻击

@安全性攻击分成两类。

@被动攻击

- @试图了解或者利用系统的信息但不影响系统资源。

@主动攻击

- @试图改变系统资源或者影响系统运行。

被动攻击

@被动攻击对传输进行窃听和监测。

@窃听：Sniffer/wiretapping/Interception

@流量分析(Traffic analysis)

- @通过对通信业务流的观察(出现、消失、总量、方向与频度)，而推断出有用的信息，比如主机的位置，业务的变化等。