



# 网络安全

## 第十章 应用程序安全加固

黄 瑋



# 温故

---

- 防火墙
  - 防外不防内
- 入侵检测
  - 防火墙的有力补充



- 防火墙和入侵检测并不能解决所有的安全加固需求
- 应用程序的安全加固是一个系统工程
- 信息安全是一个持续对抗过程

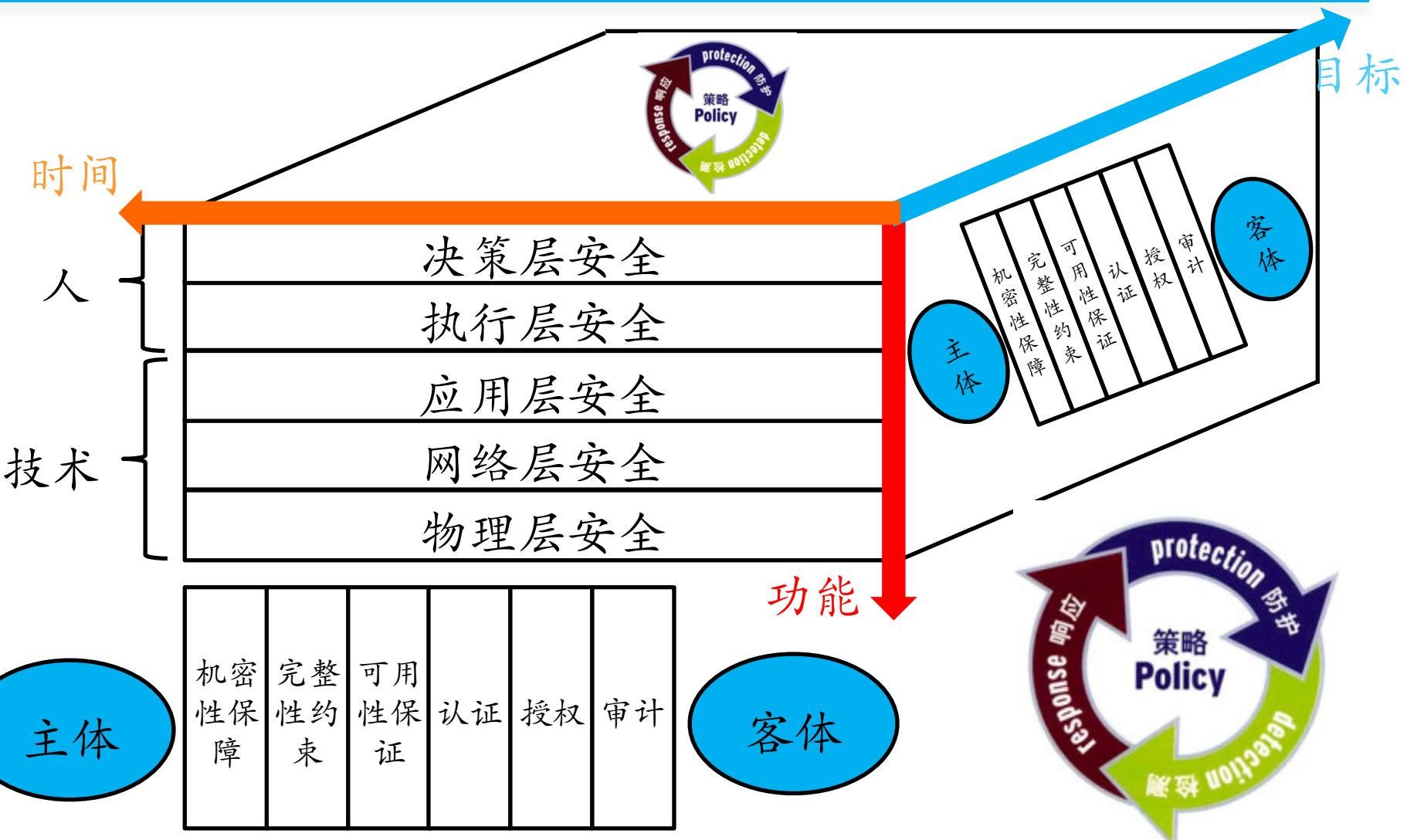


## 本章内容提要

- 信息安全技术体系与威胁模型
- 操作系统安全加固
- 应用程序安全加固
- 安全加固基准检查清单
- 安全常识科普



# 信息安全的三维技术体系





# 基于信息安全三维技术体系的安全 加固

中国传媒大学



## 功能维度——分层模型(1/5)



- 了解安全原则/常识/意义
  - 最小化授权
  - 有条件安全（没有绝对安全）
  - 木桶原理
  - 等级安全



## 功能维度——分层模型(2/5)



- 安全管理规范/安全法律/法规
  - 理解理解和掌握
  - 遵照执行



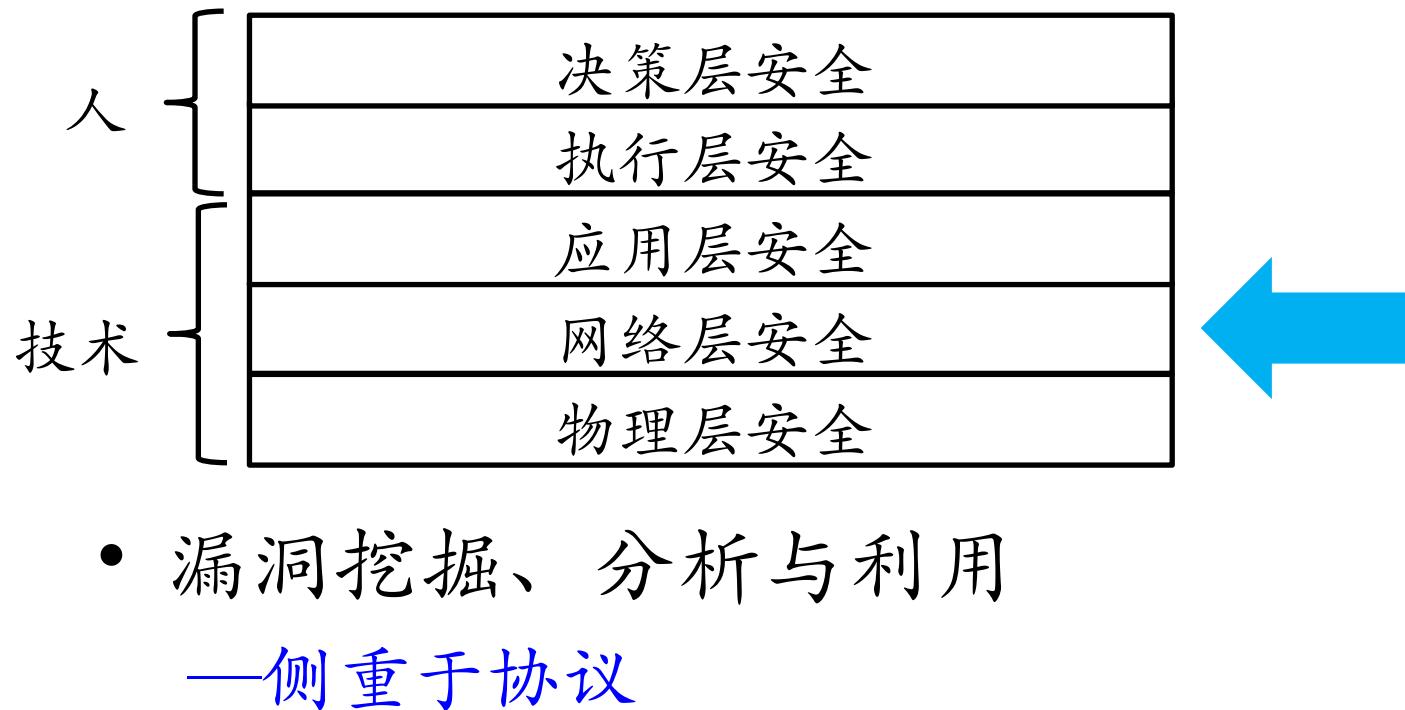
## 功能维度——分层模型(3/5)



- 漏洞挖掘、分析与利用  
—侧重于实现
- 数据/内容安全
- 运维安全



## 功能维度——分层模型(4/5)





## 功能维度——分层模型(5/5)



- IT基础设施环境安全
  - 电力供应
  - 物理环境
    - 温度、湿度、电磁辐射等



# 目标维度——访问控制模型



机密性：认证凭据的加密存储和传输，防止嗅探和复制仿冒

完整性：主体/客体/消息/信号的存储和传输不被篡改

可用性：主体随时可以访问客体

认证：验明主体真实身份

授权：验证主体有访问客体的权限

审计：防止主体抵赖对客体的历史访问



## 二维矩阵——功能+目标

	机密性	完整性	可用性	认证	授权	审计
决策层	预算拍板					
执行层	遵守执行					
应用层	文件系统 加密	主机入侵 检测系统	双机热备 系统	Ukey/动态 口令	RBAC	syslog
网络层	SSL/TLS		heartbeat	交换机的 端口接入	VPN	上网行为 监管系统
物理层	保险柜	电子安防	双线供电	门禁卡	分级门禁	视频监控



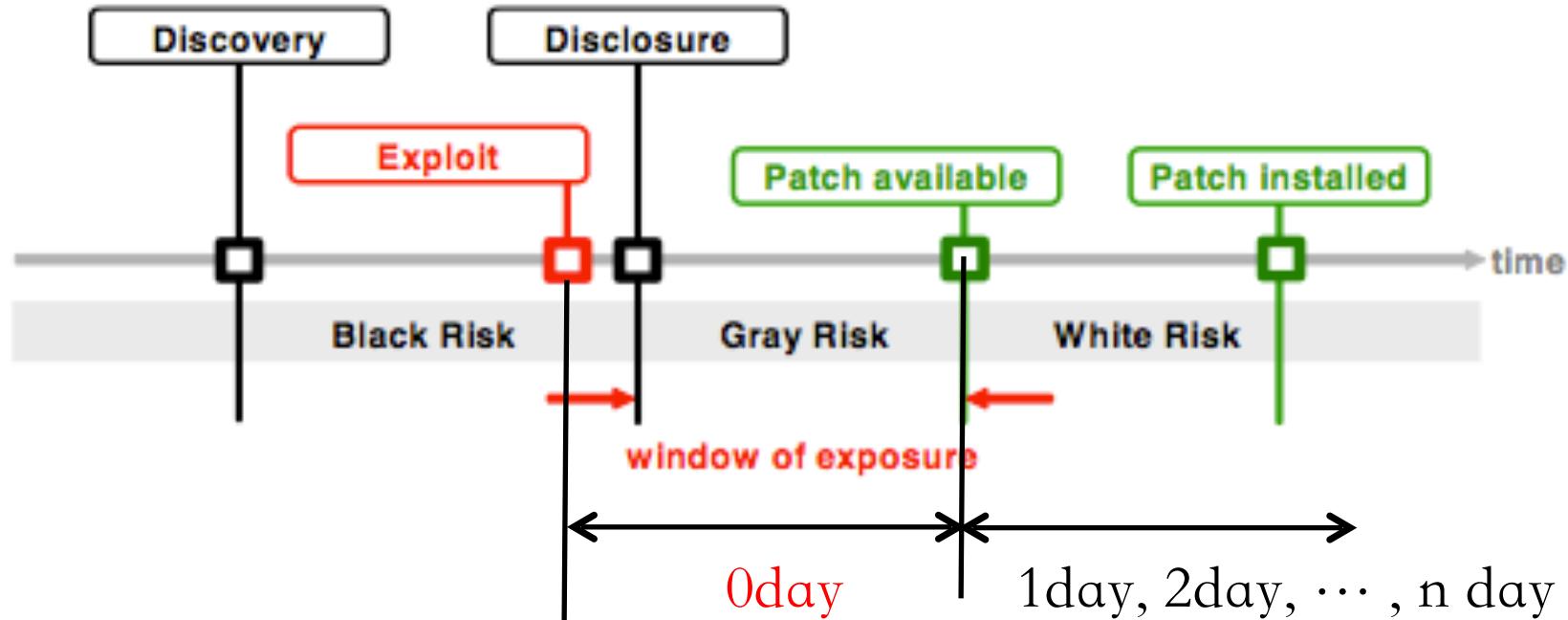
## 时间维度——P<sup>2</sup>DR模型

- 安全是
  - 持续循环过程
  - 动态变化
- 策略 (Policy)
- 防护 (Protection)
- 检测 (Detection)
- 响应 (Response)





# 认识一下0day



信息安全是一个持续对抗过程

保持自动更新是持续对抗的必然选择



# 安全加固的基本原则

- 需求驱动
  - 参考等级保护的意义
    - 明确安全需求
    - 安全防护是需要成本投入的
    - 安全建设和管理需要兼顾系统性、针对性、可行性
    - 明确重点、突出重点、保护重点
- 木桶原理
  - 安全防御中的任何一个短板都会导致整个安全防御体系的崩溃



# 安全加固的基本目标——访问控制模型

- 机密性
- 完整性
- 可用性
- 认证
- 授权
- 审计



# 安全加固的基本方法——二维矩阵

	机密性	完整性	可用性	认证	授权	审计
决策层				预算拍板		
执行层				遵守执行		风险评估/ 渗透测试
应用层	文件系统 加密	主机入侵 检测系统	双机热备 系统	Ukey/动态 口令	RBAC	syslog
网络层		SSL	heartbeat	交换机的 端口接入 认证	VPN	上网行为 监管系统
物理层	保险柜	电子安防	双线供电	门禁卡	分级门禁	视频监控

本章重点是应用层的安全加固手段介绍



## 本章内容提要

- 信息安全技术体系与威胁模型
- 操作系统安全加固
- 应用程序安全加固
- 安全加固基准检查清单
- 安全常识科普



围绕机密性目标

中国传媒大学



# 围绕机密性目标

- 需求场景分析
  - 认证凭据信息的存储
    - /etc/passwd 和 /etc/shadow
  - 配置文件中的口令信息
    - 利用 crypt(3) API 接口 加密敏感信息  
apache 的 htpasswd / proftpd 的 ftppasswd
    - 明文存储  
大量 Web 应用的配置文件
  - 加密通信



# 认证凭据信息存储机制

- 基于Hash算法

- MD5

- SHA1

- MD4

- 应用程序独立实现

- mysql

- 对称加密算法

- DES / AES



# 认证凭据信息存储机制——弱点分析(1/2)

- 基于Hash算法
  - 查表法
    - 彩虹表：Rainbow Table
- 对称加密算法
  - 密码学解密方法
- 程序实现漏洞
  - php crypt函数漏洞
    - CVE 2007-2844 php crypt function not re-entrant
    - crypt() returns only the salt for MD5 2011-08-17



# 认证凭据信息存储机制——弱点分析(2/2)

- /etc/shadow

- \$6\$**d7oTx1pP\$**sqh3ltBftJGufgbt7XPbWGaOOUDfK9zNhTVsFqi/QsZ9Uf8OQxQu7FGfwEKCzlYz17u86s1JnKsn6fCSOq5km1
- man 3 crypt**

## Glibc Notes

The glibc2 version of this function supports additional encryption algorithms.

If salt is a character string starting with the characters "\$id\$" followed by a string terminated by "\$":

\$id\$salt\$encrypted

then instead of using the DES machine, id identifies the encryption method used and this then determines how interpreted. The following values of id are supported:

ID	Method
----	--------

1	MD5
2a	Blowfish (not in mainline glibc; added in some   Linux distributions)
5	SHA-256 (since glibc 2.7)
6	SHA-512 (since glibc 2.7)



# 认证凭据信息存储机制——加固建议

- 勤打安全补丁
  - 减少程序实现漏洞
- 基于『慢速』Hash算法
  - 算法变形/混淆，相同明文密码不同hash结果
    - `password_hash()` (PHP 5.5+)
- 对称加密算法
  - 使用更安全的加密算法
    - 使用**AES / 3DES**代替脆弱的**DES**
    - 避免自己设计加密算法



# 配置文件中的口令信息

- 数据库连接配置文件
  - 数据库连接字符串中的用户名和明文口令
  - 举例
    - mediawiki 、 wordpress 等

```
17 // ** MySQL settings - You can get this info from your web host ** //
18 /** The name of the database for WordPress */
19 define('DB_NAME', 'database_name_here');
20
21 /** MySQL database username */
22 define('DB_USER', 'username_here');
23
24 /** MySQL database password */
25 define('DB_PASSWORD', 'password_here');
26
27 /** MySQL hostname */
28 define('DB_HOST', 'localhost');
29
30 /** Database Charset to use in creating database tables. */
31 define('DB_CHARSET', 'utf8');
32
33 /** The Database Collate type. Don't change this if in doubt. */
34 define('DB_COLLATE', ''');
```



# 配置文件中的口令信息——加固建议

- 加密存储敏感数据
  - 使用操作系统加密API
    - 对称加密的密钥需妥善保管
- 设置文件访问权限
  - 限制非web用户读取
  - 配置Web服务器的ACL



# 加密通信

- Open SSH
  - SSH: Secure Shell
  - SFTP: Secure File Transfer Protocol
  - XXX over SSH
    - svn over ssh
    - git over ssh
- VPN
  - 见《第三章 网络安全应用基础》



# 加密通信——弱点分析

- 协议设计缺陷
  - SSL 1.0, 2.0, 3.0 / TLS 1.0 (SSL 3.1)
- 协议实现漏洞
  - New Tricks For Defeating SSL in Practice blackhat-dc-2009
  - OpenSSL cipher downgrade attack (CVE-2010-4180)
  - Padding Oracle Crypto Attack 2010.09
  - BEAST attack on TLS 1.0 (SSL 3.1) 2011.09
  - Heartbleed attack on OpenSSL CVE-2014-0160 2014.4
  - Poodle: SSLv3 vulnerability CVE-2014-3566 2014.11
- 网络环境漏洞
  - 见《第四章 网络监听》



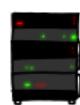
# Heartbleed漏洞原理与危害

## HOW THE HEARTBLEED BUG WORKS:

SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "POTATO" (6 LETTERS).



User Meg wants these 6 letters: POTATO. User Isabella wants pages about "irl games". Unlocking secure records with master key 5130985733433433... User Olivia wants pages about "bees in car why". Note: Files for IP 375.381.383.17 are in /tmp/files-3843.



User Olivia from London wants pages about "bees in car why". Note: Files for IP 375.381.383.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file telefiring (contents: 33ba962e2cab9ff89b43bfef8)



User Meg wants these 6 letters: POTATO. User Isabella wants pages about "irl games". Unlocking secure records with master key 5130985733433433... User Olivia wants pages about "bees in car why". Note: Files for IP 375.381.383.17 are in /tmp/files-3843.

POTATO



SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "HAT" (500 LETTERS).



User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CofBaSt". User Jake requested pictures of deer



SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "BIRD" (4 LETTERS).



User Olivia from London wants pages about "bees in car why". Note: Files for IP 375.381.383.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 346 connections open. User Brendan uploaded the file telefiring (contents: 33ba962e2cab9ff89b43bfef8)



User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CofBaSt". User Jake requested pictures of deer



攻击者可以读取启用了SSL/TLS加密的服务器内存里的任意数据，包括但不限于：SSL加密私钥、用户cookie等



# 加密通信——加固建议

- 使用已被验证安全可靠的加密协议
  - 禁用存在已知协议漏洞的加密协议
- 勤打安全补丁
  - 减少程序实现漏洞
- 做好网络通信基础设施安全加固
  - 见《第四章 网络监听》



围绕完整性目标

中国传媒大学



## 围绕完整性目标(1/2)

- 需求场景分析
  - 文件完整性签名
    - 确保文件来源的可信
    - 确保文件未被非法篡改
  - 防篡改解决方案
    - 网页防篡改
    - 数据库防篡改
  - 运行时完整性
  - 通信过程完整性



## 围绕完整性目标(2/2)

- 运行时完整性检查
  - 资源载入
    - 第三方库加载（例如dll加载污染漏洞）
  - 内存变量
    - 慎用全局变量存储敏感数据
  - API调用
    - API hook检查
- 通信过程完整性
  - SSL / VPN / IPSec等
  - 应用层完整性校验



# 主流网页防篡改技术举例

	外挂轮询技术	事件触发技术	核心内嵌技术
访问篡改网页	可能	可能	不可能
保护动态内容	不能	不能	能
服务器负载	中	低	低
带宽占用	中	无	无
检测时间	分钟级	秒级	实时
绕过检测机制	不可能	可能	不可能
防范连续篡改攻击	不能	不能	能
保护所有网页	不能	能	能
动态网页脚本	不支持	支持	支持
适用操作系统	所有	受限	所有
上传时检测	不能	受限	能
断线时保护	不能	不能	能



围绕可用性目标



## 围绕可用性目标

- 需求场景分析
  - 数据备份
  - 业务备份
  - 备份还原测试
  - 负载均衡
    - 基于域名
    - 基于应用层协议
    - 基于后端计算/存储/带宽资源
  - 防DoS/DDoS



围绕认证目标

中国传媒大学



## 围绕认证目标(1/3)

- 需求场景分析

- 身份识别

- 身份集合

- 普通用户 / bot / 管理员 / API

- 精确度 (唯一性标识的粒度)

- 身份验证

- 验证强度

- 易用性和安全性的平衡



## 围绕认证目标(2/3)

- 单因素认证加固
  - 强制口令安全策略
    - 口令强度限制  
    口令长度/口令复杂度
    - 口令生命周期  
    定期更换口令



## 围绕认证目标(3/3)

- 双因素/多因素认证
  - know / has / is /where
- CAPTCHA机制防止自动化暴力破解认证
  - 图片验证码
  - 音频验证
  - 客户端图灵测试
    - Web浏览器的客户端js代码执行



围绕**授权**目标

中国传媒大学



## 围绕授权目标(1/3)

- 需求场景分析
  - 已认证用户的滥用/误用行为
  - 代码漏洞导致的任意指令执行/任意资源访问
  - 可靠的授权变更机制
    - 取消授权
    - 新授权
    - 变更授权



## 围绕授权目标(2/3)

- 最小化授权
  - 认证用户的权限分配
  - 代码执行的权限分配
    - 沙盒机制
    - jailed机制
  - 最小化安装和配置
    - 删除/禁用所有非必需服务/应用



## 围绕授权目标(3/3)

- 取消授权
  - 取消已认证的身份数字标识
    - 取消绑定的资源/权限
- 新授权
  - 新建主体和客体
  - 新建主体对客体的访问授权（关联）
- 变更授权
  - 变更主体对客体的访问授权（关联）



围绕审计目标

中国传媒大学



## 围绕审计目标(1/2)

- 需求场景分析
  - 入侵取证
  - 历史行为审计
    - 面向用户
    - 面向资源



## 围绕审计目标(2/2)

- 日志系统的CIA加固
  - 机密性：避免记录敏感信息，如认证凭据
  - 完整性：日志系统防篡改
  - 可用性：
    - 日志系统的持续可用
    - 避免海量日志耗尽磁盘存储
      - 正确配置应用程序日志的轮转策略
      - iptables的conntrack资源耗尽问题
- 自动化审计
  - 自动分析日志
  - 主机入侵检测



# 操作系统安全加固小结

中国传媒大学



# 操作系统安全加固小结

- CIA+AAA是安全加固的基本目标
- 操作系统安全加固是所有安全加固的基础
  - 应用程序
  - 网络通信
  - 人的安全意识/安全（执行）能力
- 操作系统安全加固的原则和经验是
  - 可借鉴
  - 可推广
  - 可移植



## 本章内容提要

- 信息安全技术体系与威胁模型
- 操作系统安全加固
- 应用程序安全加固
- 安全加固基准检查清单
- 安全常识科普



# 应用程序安全加固

- Web
- SSH
- DNS



# 用分层的方法来看Web威胁模型

详见第七章





# Web安全加固目标概述

- 基于操作系统安全加固策略
  - 针对Web应用程序漏洞分类进行代码级别加固
    - 参考《第六章 网络与系统渗透》
  - 服务器软件配置加固
    - 代理服务器
    - Web服务器
    - 应用服务器
    - 数据库服务器
- 借鉴操作系统安全加固的原则和经验



# 服务器软件配置加固——代理服务器

- 反向代理的敏感信息泄漏
  - 正确配置URL匹配规则并自定义错误信息页面
    - 避免通过枚举方式发现反向代理服务器  
创新工厂安全宝信息泄漏漏洞洞
- 正向代理的身份认证
  - 限制或禁用匿名代理服务
    - 避免被滥用于非法入侵的跳板  
iku爱酷后台开放匿名代理服务



# 服务器软件配置加固——Web服务器

- 敏感信息泄漏
  - 自定义错误信息页面
  - 生产环境服务器屏蔽显示debug详细信息
  - 禁止特定扩展名文件的直接访问
    - 黑名单：.bak/.exe/.config/.txt/.htaccess等
- 通信完整性保护
  - 正确配置https
    - 使用权威CA颁发的SSL证书
    - 避免自签发



# 服务器软件配置加固——Web服务器

- 软件完整性保护
  - 网页防篡改
- AAA加固
  - 避免使用Basic认证保护重要系统入口
    - 防止暴力破解
  - 日志系统加固
    - 参考操作系统日志加固策略
- 纵深防御
  - 部署于DMZ
    - 强化内网安全，避免 DMZ↔内网 的访问



# 服务器软件配置加固——应用服务器

- 最小化授权
  - 代码可执行目录限制
    - 取消上传目录和临时目录等的代码执行权限
  - 可写目录限制
    - 取消非上传目录的写入权限
  - 其他沙盒机制
- 敏感信息泄漏
  - 同Web服务器加固策略
- 部署WAF



# WAF之mod\_security(1/4)

- 功能特性
  - HTTP流量记录
  - 实时监控和攻击检测
  - 攻击防护和虚拟补丁
    - 黑名单/白名单/已知弱点和漏洞（规则）
  - 灵活的（检测和响应）规则引擎
  - 支持嵌入式部署
  - 支持网络部署
  - 跨平台支持



## WAF之mod\_security(2/4)

- OWASP ModSecurity CRS Project
  - Core Rule Set
    - HTTP防护
    - 常见Web攻击防护
    - 自动化检测
    - 木马防护
    - 错误消息隐藏
  - 配置方法
    - [http://sourceforge.net/apps/mediawiki/mod-security/index.php?title=Reference\\_Manual](http://sourceforge.net/apps/mediawiki/mod-security/index.php?title=Reference_Manual)

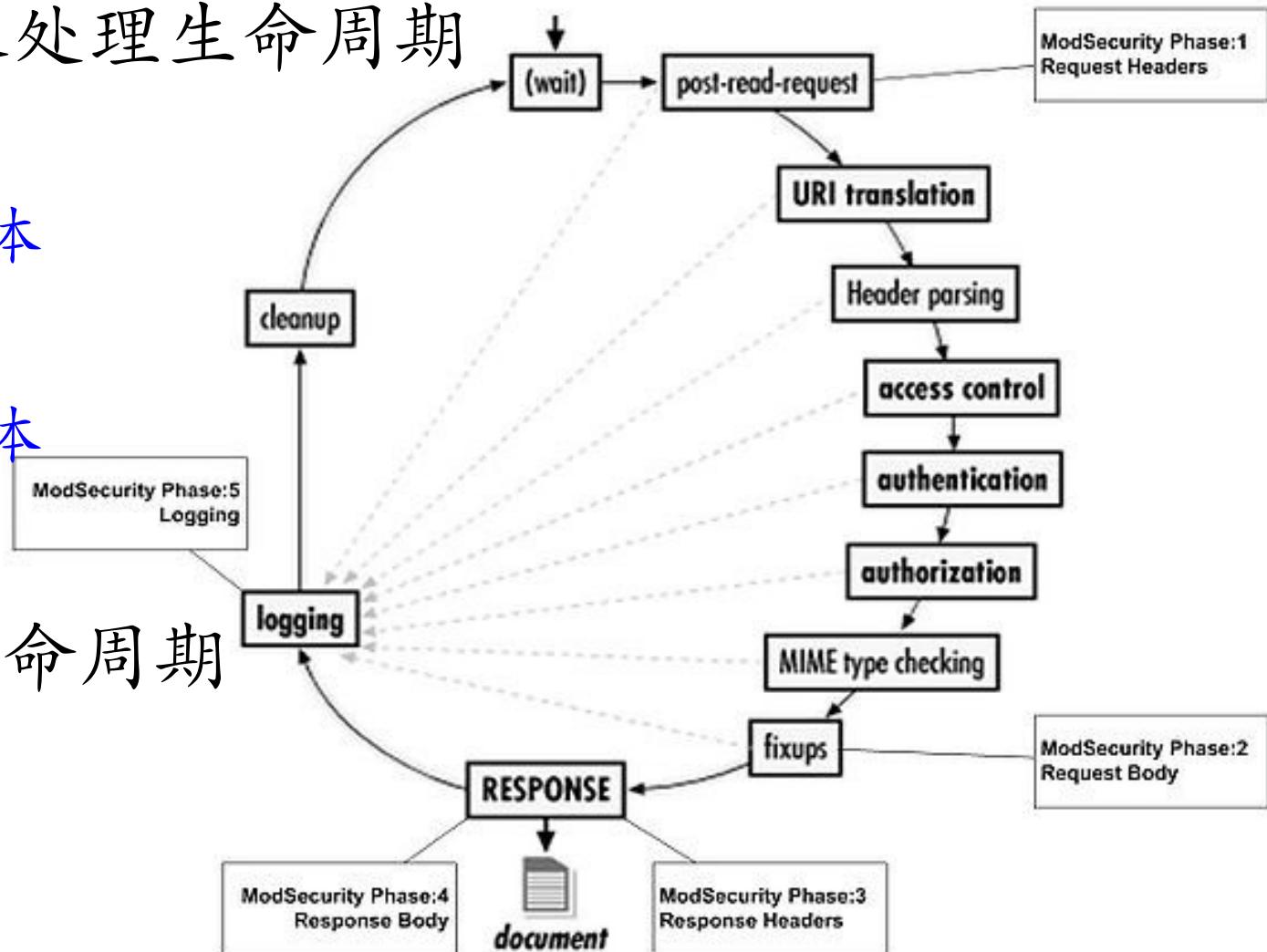


## WAF之mod\_security(3/4)

- Apache请求处理生命周期

- 请求头部
- 请求消息体
- 响应头部
- 响应消息体
- 日志

- 完整覆盖生命周期





# WAF之mod\_security(4/4)

- 典型规则应用

- 拒绝SQL注入:

- SecFilter "delete[:space:]]+from"
    - SecFilter "insert[:space:]]+into"
    - SecFilter "select.+from"

- 拒绝Googlebot访问

- SecFilter HTTP\_USER\_AGENT "Google" nolog,redirect:http://www.google.com

- 拒绝特定命令执行

- SecFilter /etc/password
    - SecFilter /bin/ls

- 拒绝目录遍历

- SecFilter "\.\./"



## 其他Apache安全加固相关模块

- mod\_evasive
  - 防DoS/DDoS
  - <http://library.linode.com/web-servers/apache/mod-evasive>
- mod\_bandwidth
  - 并发连接数和带宽限制



通用应用层防火墙

基于主机的入侵防御系统-fail2ban



## 概述

- 官方网站：[http://www.fail2ban.org/wiki/index.php/Main\\_Page](http://www.fail2ban.org/wiki/index.php/Main_Page)
- 版本
  - 0.8.x / 0.9.x
- 典型应用场景
  - 防止(帐号)穷举/破解类攻击



# 基本原理

- 监控日志文件，检索设定的访问指纹（正则表达式），匹配指纹成功后
  - 统计指定时间内的匹配次数
  - 超出设定的频率阈值时，执行预定的响应策略（可组合）
    - 设置防火墙规则屏蔽访问来源
      - 可指定屏蔽时长，过期自动解封
    - 发送邮件通知系统管理员
    - 记录日志到syslog



# 典型的Linux系统日志

- /var/log/auth (Debian/Ubuntu)
- /var/log/secure (Fedora)
- /var/log/apache2/error.log
- /var/log/nginx/error.log



# Fail2ban基本概念

- filter
  - 异常访问行为的正则表达式规则
  - 软件有内置规则，也可自定义
- action
  - 策略匹配成功时可执行的响应命令(集合)
  - 典型响应命令就是将来源IP添加到iptables的禁止规则
- jail
  - filter和action策略集合



# fail2ban配置

- /etc/fail2ban/
  - action.d/                   **action**规则目录，可自行添加新规则文件到该目录下(.conf结尾)
  - filter.d/                   **filter**规则目录，可自行添加新规则文件到该目录下(.conf结尾)
  - fail2ban.conf               系统默认全局参数配置规则文件
  - jail.conf                   系统默认**jail**配置规则文件
  - jail.local                  用户自定义**jail**配置规则文件，需自行创建



# fail2ban配置调试

```
root@kali-local:/etc/fail2ban# cat filter.d/apache-anti-enum-scan.conf
[INCLUDES]
before = apache-common.conf
[Definition]
failregex = ^%(_apache_error_client)s File does not exist: .*$
ignoreregex = ^%(_apache_error_client)s File does not exist: .*\.ico$
```

```
root@kali-local:/etc/fail2ban# cat jail.local
[DEFAULT]
action=%(action_mwl)s
ignoreip = 127.0.0.1
bantime = 60
maxretry = 10
findtime = 60

[apache-anti-enum]
enabled = true
port    = http,https
filter = apache-anti-enum-scan
logpath = /var/log/apache2/error.log
```



# fail2ban配置调试与测试

```
root@kali-local:/etc/fail2ban# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
fail2ban-apache-anti-enum  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
fail2ban-ssh    tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 22

Chain FORWARD (policy ACCEPT)
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination

Chain fail2ban-apache-anti-enum (1 references)
target     prot opt source          destination
RETURN    all  --  0.0.0.0/0            0.0.0.0/0

Chain fail2ban-ssh (1 references)
target     prot opt source          destination
RETURN    all  --  0.0.0.0/0            0.0.0.0/0
root@kali-local:/etc/fail2ban#
```

```
1. root@kali-local: /etc/fail2ban (ssh)
root@kali-local:/etc/fail2ban# fail2ban-regex /var/log/apache2/error.log
/etc/fail2ban/filter.d/apache-anti-enum-scan.conf /etc/fail2ban/filter.d/
apache-anti-enum-scan.conf

Running tests
=====

Use ignoreregex file : /etc/fail2ban/filter.d/apache-anti-enum-scan.conf
Use regex file : /etc/fail2ban/filter.d/apache-anti-enum-scan.conf
Use log file   : /var/log/apache2/error.log

Results
=====
Failregex
|- Regular expressions:
|  [1] ^\[[^\]]+\] \[error\] \[client <HOST>\] File does not exist: .*$
|
`- Number of matches:
  [1] 119 match(es)

Ignoreregex
|- Regular expressions:
|  [1] ^\[[^\]]+\] \[error\] \[client <HOST>\] File does not exist: .*.ico
$ 
|
`- Number of matches:
  [1] 21 match(es)

Summary
```



# fail2ban-client

```
root@kali-local:/etc/fail2ban# fail2ban-client status
Status
|- Number of jail:      2
`- Jail list:          ssh, apache-anti-enum
root@kali-local:/etc/fail2ban# fail2ban-client status ssh
Status for the jail: ssh
|- filter
| |- File list:        /var/log/auth.log
| |- Currently failed: 0
| `- Total failed:     0
`- action
  |- Currently banned: 0
  | `- IP list:
  `- Total banned:     0
root@kali-local:/etc/fail2ban# fail2ban-client status apache-anti-enum
Status for the jail: apache-anti-enum
|- filter
| |- File list:        /var/log/apache2/error.log
| |- Currently failed: 0
| `- Total failed:     0
`- action
  |- Currently banned: 0
  | `- IP list:
  `- Total banned:     0
root@kali-local:/etc/fail2ban#
```



# fail2ban配置测试

```
root@kali-local:/etc/fail2ban# fail2ban-client status
Status
|- Number of jail:      2
`- Jail list:          ssh, apache-anti-enum
root@kali-local:/etc/fail2ban# fail2ban-client status apache-anti-enum
Status for the jail: apache-anti-enum
|- filter
| |- File list:        /var/log/apache2/error.log
| |- Currently failed: 0
| `-- Total failed:    26
`- action
  |- Currently banned: 1
  | |- IP list:         192.168.56.1
  | `-- Total banned:   2
root@kali-local:/etc/fail2ban# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
fail2ban-apache-anti-enum  tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
fail2ban-ssh    tcp  --  0.0.0.0/0            0.0.0.0/0           multiport dports 22

Chain FORWARD (policy ACCEPT)
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination

Chain fail2ban-apache-anti-enum (1 references)
target     prot opt source          destination
DROP      all  --  192.168.56.1       0.0.0.0/0
RETURN    all  --  0.0.0.0/0       0.0.0.0/0

Chain fail2ban-ssh (1 references)
```



# 服务器软件配置加固——数据库服务器

- 最小化授权
  - 限制数据库的入站连接
    - 基于白名单的数据库客户端连接
  - 限制数据库连接用户权限
    - 禁用管理员授权
    - 禁用所有非必需数据库应用扩展
      - 禁用危险的存储过程/UDF等
    - 只授予必需权限
- 部署数据库防火墙



# 应用程序安全加固

- Web
- SSH
- DNS



# SSH安全加固一二三

- 更换默认的SSH监听端口
- sshd配置安全加固

- 使用第三方安全加固工具

— 防止口令暴力破解

- fail2ban
- denyhosts
- pam\_abl

```
# 建议更换默认端口  
Port 22  
# 建议只监听需要的端口，默认是监听所有可用的本机IP地址  
#ListenAddress ::  
#ListenAddress 0.0.0.0  
# 建议只使用SSH协议版本2  
Protocol 2  
# 建议使用更长的服务器密钥长度，如2048  
ServerKeyBits 768  
# Authentication:  
# 默认登录超时时间为120秒，建议缩短该时间到30  
LoginGraceTime 120  
# 建议禁止Root用户直接登录，将yes改为no  
PermitRootLogin yes  
# 如果你不需要基于口令的登录方式，可以将yes改为no  
#PasswordAuthentication yes
```



# 应用程序安全加固

- Web
- SSH
- DNS



# DNS安全加固一二三(1/2)

- 使用DNSSEC
  - 基于PKI体系对抗
    - DNS缓存污染
    - DNS域名劫持
    - DNS解析重定向
- 敏感信息泄漏
  - 正确配置以杜绝Zone Transfer
    - 内网信息泄漏



## DNS安全加固一二三(2/2)

- AAA加固
  - 域名注册服务提供商的管理帐号安全
    - 口令安全
    - 防止社会工程学攻击
  - 恶意篡改域名解析配置



## 本章内容提要

- 信息安全技术体系与威胁模型
- 操作系统安全加固
- 应用程序安全加固
- 安全加固基准检查清单
- 安全常识科普



# 公开标准

- Google “security checklist”
- XCCDF
  - The Extensible Configuration Checklist Description Format by NIST
- 切忌教条式照搬已有的安全加固基准清单
  - 因地制宜
    - 业务需求
    - 运行环境
    - 管理制度



## 本章内容提要

- 信息安全技术体系与威胁模型
- 操作系统安全加固
- 应用程序安全加固
- 安全加固基准检查清单
- 安全常识科普



# 信息安全知识科普与应用

- 安全常识
- 社交应用使用守则
- 常用软件
- 不可忽视的细节



## 图标说明



- 危险意识/行为



- 科普意识/行为



- 提倡意识/行为



## 安全常识

i

- 安全的本质是持续对抗



- 自动更新



- 使用最新版软件

i

- 安全防御的倒金字塔现象和木桶原理

i

- 天上不会掉馅饼

- 无事献殷勤：非奸即盗

i

- 保密原则

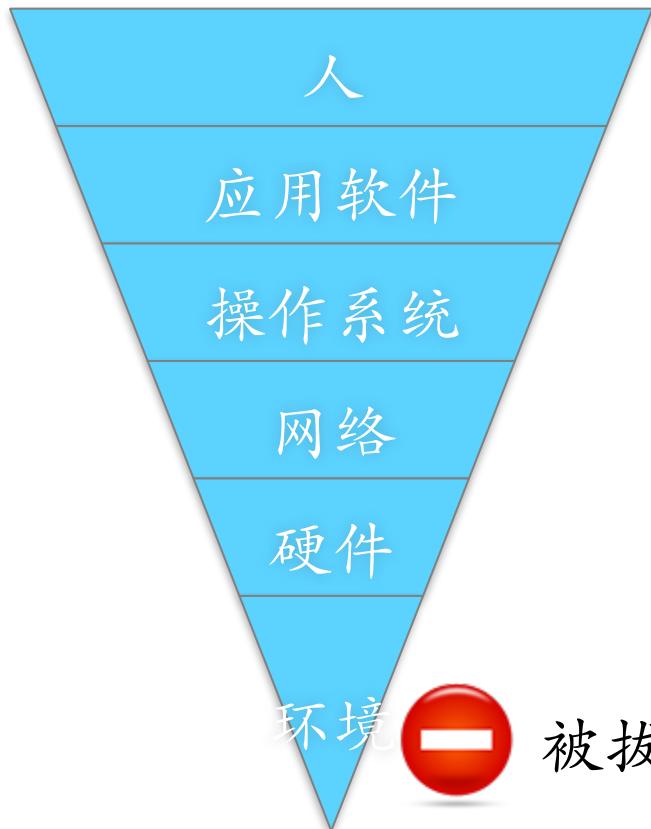
i

- 千里之堤毁于弱口令



# 安全防御的倒金字塔现象

- 底层安全程度决定上层安全的稳固性



弱口令/记住口令功能/无视安全警告  
用Excel、Word、记事本管理密码  
用QQ、电子邮件发送口令



自动更新



使用最新版软件



被拔网线/外来人员的偷拍



# 安全防御的木桶原理

- 整体安全防御的能力高低取决于最短板的高度





# 天上不会掉馅饼



- 恭喜您，中奖了！



—“把你公司的员工通讯录发给我吧”



—“这是礼品目录，下载查看吧”



- 恭喜您获得了我们公司的试用体验机会



—“我们将派工作人员上门登记你们公司的员工信息，以便准备足够数量的试用套装”



- XXX大优惠



—话费冲300返600



—10MB带宽XXX元



## 保密原则



- 我借用一下你们公司的
  - 电脑 / 无线网络 / 有线网络



- 公司 **内**任何形式的资料未经允许
  - 不得对外传播
  - 不得私自携带外出
  - 不得私自存储和备份
    - 纸质文件
    - 源代码 / 电子文档 / 会议纪要 / 电子邮件 / 产品概念图 / 研发计划 / 薪酬待遇 …



## 千里之堤毁于弱口令 (1/4)

- 你在用这些弱口令吗？



—手机号



—公司/住宅电话号码



—生日



—123456 / 888888 / 1qaz2wsx / asdf

- 你的口令都是怎么记忆的？



—使用软件自带的“记住密码”功能



—新建一个文本文件



—记在一个本子上



## 千里之堤毁于弱口令 (2/4)

- 强口令就真的很强吗?
  - ba1f2511f
  - 手机号+手机号
  - 手机号+生日
- 如果你的人人网账号被盗，你的QQ账号还保得住吗?
  - 单一口令也是弱口令



# 千里之堤毁于弱口令 (3/4)

- 口令是信息安全的安全底座
  - 口令被盗即意味着安全大厦的根基被毁
- 口令的强度和记忆难度的平衡
  - 无规则随机产生的口令是无法记忆的
  - 记忆友好强口令产生规则
    - 使用短语/长句（拼音首字母/全拼）
      - 系列人名/古诗词等等
    - 使用独立口令
      - 使用更“安全”的密码管理软件
      - 自定义一套不同站点/应用的口令派生规则



# 千里之堤毁于弱口令 (4/4)

- 口令被盗的原因
  - 主机中病毒/木马
    - 键盘输入截获
    - 软件“已保存/已记住”的口令被解密/提取
  - 被“钓鱼”
  - 口令的网络传输使用明文
  - 第三方站点/应用被黑客攻陷
    - “加密”口令被黑客解密
    - 黑客使用A站点解密出的用户名+口令组合去尝试登录B/C/D…站点/应用



# 强口令很了不起吗？

- 找回口令功能

- 密码提示问题



- 你爸爸/妈妈的名字?



- 你高中时的学校名字?



- 你的第一任班主任姓名?



- 你是如实回答以上问题的吗?

- 发送口令重置链接到你的邮箱

- 你的邮箱口令也是强口令吗?

你的邮箱的找回口令功能足够安全吗?

...



# 社交应用使用原则



晒照片



位置签到



好友公开互动

公开的就不再有隐私！

还记得前面刚讲过的口令安全问题吗？





# 常用软件

---

- 浏览器
- 办公软件
- 即时通讯
- 电子邮件
- 下载和安装软件
- 安全软件



## 浏览器



- 记住口令功能



- URL



- 地址栏



- 页面内的链接

——短网址



- 使用现代浏览器





## 浏览器——记住口令功能



- 黑客可以从浏览器中提取出保存的口令



- 禁用浏览器的口令保存功能



- 删 除已经保存的口令



- 定期清空所有浏览历史记录数据



## 社会工程学手段

- URL混淆欺骗
- 仿冒页面
- XSS跨站点脚本欺骗
- 虚假邮件内容钓鱼
- 虚假邮件信任关系钓鱼
- IM欺诈



# 社会工程学手段——URL混淆欺骗

- 二级/三级域名： news.baidu.xxx.com != baidu.com
  - URLEncode编码：

www.baidu%74%65%73%74.com -----»  
www.baidutest.com

- 相似字母/数字：
  - www.micros0ft.com
  - www.1enovo.com



# 社会工程学手段——URL混淆欺骗

- IP地址编码
  - `http://3546189924 -----» http://211.94.144.100 -----» http://www.baidu.com`
  - `http://0xd3.0x5e.0x90.0x64 -----» http://211.94.144.100 -----» http://www.baidu.com`
- Web应用程序重定向Bug
  - Google的“手气不错”任意URL重定向漏洞：  
`http://www.google.com/search?btnI&q=site:http://www.yahoo.cn`



# 社会工程学手段——URL混淆欺骗

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\huangwei>ping 3546189924

Pinging 211.94.144.100 with 32 bytes of data:

Reply from 211.94.144.100: bytes=32 time=210ms TTL=51

Ping statistics for 211.94.144.100:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 210ms, Maximum = 210ms, Average = 210ms
Control-C
^C
C:\Documents and Settings\huangwei>ping 0xd3.0x5e.0x90.0x64

Pinging 211.94.144.100 with 32 bytes of data:

Reply from 211.94.144.100: bytes=32 time=102ms TTL=51

Ping statistics for 211.94.144.100:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 102ms, Maximum = 102ms, Average = 102ms
```



# 社会工程学手段——URL混淆欺骗

- 防范方法：
  - Firefox 3+/IE 7&8的仿冒网站过滤功能
  - 鼠标悬停于链接上，看浏览器左下角的状态栏信息
  - 最简单、准确的方法：域名->IP解析



# 社会工程学手段——仿冒页面

Screenshot of a fake Tencent公益网 (Tencent Charity Network) website.

The URL in the address bar is [http://www.qq.com/indexq\\_cn/news/news\\_qq\\_com/a/20080512/index.htm](http://www.qq.com/indexq_cn/news/news_qq_com/a/20080512/index.htm).

The page features a red heart logo for "Tencent公益网 GONGYI.NET".

Navigation menu items include: 首页 (Home), 公益资讯 (Public Welfare Information), 志愿者部落 (Volunteer Tribe), 公益联盟 (Public Welfare Alliance), 正在捐赠 (Currently Donating), 爱心义卖 (Charity Sale), and 帮助与指引 (Help and Guidance).

A banner headline reads: "腾讯公益慈善基金会联合中国红十字总会李连杰壹基金计划为5.12四川地震紧急募捐" (Tencent Charity Foundation and China Red Cross Society, together with Li Lianjie's壹基金, plan to raise funds for the May 12 Sichuan Earthquake emergency relief).

The banner includes a map of Sichuan showing the震中 (epicenter) near Mianyang, and several images of people in disaster relief efforts.

The main content area discusses the May 12 earthquake and the foundation's response:

北京时间5月12日14时28分，四川汶川县发生了里氏7.8级地震。胡锦涛总书记立即作出重要指示，要求尽快抢救伤员，保证灾区人民生命安全，温家宝总理也迅速赶赴灾区指导救灾工作。

在全国上下同心协力抗震救灾的同时，腾讯公益慈善基金会第一时间启动紧急救援机制，首批

A sidebar titled "最新在线捐款人" (Latest Online Donors) lists two recent donations:

最新在线捐款人	金额	时间
1 李忠盛	100元	5小时前
2 牛牛一家	100元	5小时前



# 社会工程学手段——XSS跨站点脚本欺骗





# 社会工程学手段——XSS跨站点脚本欺骗





# 社会工程学手段——XSS跨站点脚本欺骗

- 防范方法：
  - IE 8的新增安全机制XSS Filter
  - Firefox的扩展：
    - NoScript：可以过滤XSS、CSRF等多种针对浏览器的移动脚本攻击
    - FireKeeper：浏览器里的IDS，实时监控分析Web服务器和浏览器之间的通信流量



## 办公软件 (1/2)

- 微软Office系列
  - 禁用宏
- PDF
  - 使用第三方PDF阅读器
    - Foxit
- 不打开来历不明的文档
- 不要被“图标”迷惑
  - 应用程序图标是可以被伪造的
    - 一个具有Word图标的文件可以是.exe伪装的



## 办公软件 (2/2)

- 不要被“扩展名”迷惑
  - 使用大量空格填充可以轻松“伪造”任意扩展名
    - 如果再使用自定义的文件“图标”呢?



- 通过异常的文件大小来识别一些恶意文档
  - 3MB的简历文档（正常简历大小在50KB左右）
- 使用Web版邮箱中的在线查看文档功能
  - 尽量不要下载简历后在本地打开查看



# 社会工程学手段——IM 欺诈

- QQ尾巴病毒
- 虚假中奖消息
- 伪造聊天视频



## 即时通讯——QQ

- 视频欺诈
- 恶意文件
- 恶意链接
- 不和陌生人说话
- 熟人之间不谈“不熟”之事  
——借钱/询问口令/询问帐号



# 电子邮件

- 钓鱼邮件
  - 伪造发信人
  - 伪造内容
    - 邮件发信人昵称/邮件标题/邮件正文
- 邮件附件中的病毒和木马
- 重要资料不通过邮件发送和讨论
  - 内网传输和讨论
- 重要行动前，电话/当面再确认行动内容
  - 收到陌生邮件通知：“XXX，我更换了邮箱地址，请惠存”



# 社会工程学手段——虚假邮件内容钓鱼

- Gmail钓鱼示例：

尊敬的用户：

您的Gmail帐号由于非正常的操作即将被封锁,这可能由以下原因引起:

1. 在短时间内接收、删除或下载大量邮件 (透过 POP)。
2. 发送大量无法寄送的邮件 (退回的邮件)。
3. 使用文件分享或文件存储软件、浏览器扩展组件或会自动登录您帐号的第三方软件。
4. 您的Gmail帐户有多个操作处于开启状态。
5. 与浏览器相关的问题。请注意，如果您发现浏览器在尝试存取您的收件箱时会持续重新载入，这很可能是浏览器的问题，而且可能需要清除您浏览器的快照和Cookie。

为不影响您的正常使用，请在以下窗口重新验证您的帐号信息：

Google 帐号  
验证

用户名:

密码:

在此电脑上记录我的登录信息。



# 社会工程学手段——虚假邮件内容钓鱼

尊敬的用户：

您的Gmail帐号由于非正常操作即将被封锁，这可能由以下原因引起：

1. 在短时间内接收、删除或下载大量邮件 (透过 POP)。
2. 发送大量无法寄送的邮件 (退回的邮件)。
3. 使用文件分享或文件存储软件、浏览器扩展组件或会自动登录您帐号的第三方软件。
4. 您的Gmail帐号有多个操作处于开启状态。
5. 与浏览器相关的问题。请注意，如果您发现浏览器在尝试存取您的收件箱时会持续重新载入，这很可能是浏览器的问题，而且可能需要清除您浏览器的快照和Cookie。

为不影响您的正常使用，请在以下窗口重新验证您的帐号信息：

Google 帐号  
验证

用户名:

密码:

在此电脑上记录我的登录信息。



# 社会工程学手段——虚假邮件内容钓鱼

- 防范方法：
  - SMTP服务器配置严格的垃圾邮件过滤程序
  - 用户要提高安全意识，要仔细检查发信人地址。



# 社会工程学手段——虚假邮件信任关系钓鱼

- 伪造发信

- 利用收件人对发信人真实性的信任关系，诱骗收信人点击链接、下载执行文件或提交隐私信息等

- SMTP服务器配置漏洞
    - 中毒主机



# 社会工程学手段——虚假邮件信任关系钓鱼

- Yahoo Mail钓鱼示例：

电邮 地址簿 效率手册 记事本 邮箱设置

收信 写信 变身金领的秘密 搜索电邮 网上搜索

新版订阅全面上线 切换到新的Yahoo! 邮箱

收件箱 查看：所有邮件 75封邮件中的 26-50 第一页 | 上一页 | 下一页 | 最后一页

文件夹 [添加 - 编辑]

发件人	主题	日期	大小
CPNTools@daimi.au.dk	CPN Tools license	2008年4月22日 (二)	3k
InfoQ中文站	Java漢硅薄鐵很熊鑄◆ - 滑懈la Bini涓€璧峰帰璁↗Ruby - RESTful涓榕晫閭出殑Cool URL...	2008年4月22日 (二)	20k
admin@yahoo.cn	系统管理员通知	2008年4月22日 (二)	1k
admin@yahoo.cn	系统管理员通知	2008年4月21日 (一)	1k
admin@yahoo.cn	系统管理员通知	2008年4月21日 (一)	1k
admin@yahoo.cn	系统管理员通知	2008年4月21日 (一)	1k
admin@yahoo.cn	系统管理员通知	2008年4月21日 (一)	1k
admin@bupt.edu.cn	系统管理员通知	2008年4月21日 (一)	1k

收件箱 草稿 已发送邮件 垃圾邮件 (2) [清空] 已删除邮件 [清空] 我的文件夹 [隐藏] 支付凭证 注册信息 搜索快捷键 我的照片



# 社会工程学手段——虚假邮件信任关系钓鱼

- 防范方法

- 查看邮件原始信息
- SMTP服务器增加对发信人源地址的身份认证
- 用户身份认证：发信人源地址域名 → IP地址解析验证
- 服务器端部署反垃圾邮件系统
  - 邮箱域名签名
  - 基于PKI的
    - 域名防伪造
    - 邮箱地址防伪造



# 社会工程学手段——虚假邮件信任关系钓鱼

电邮 地址簿 效率手册 记事本 邮箱设置

收信 写信 变身金领的秘密 搜索电邮 网上搜索

新版订阅全面上线

文件夹 [添加 - 编辑]

收件箱  
草稿  
已发送邮件  
垃圾邮件 [未空]  
已删除邮件 [未空]

我的文件夹  
支付凭证  
注册信息  
隐藏

搜索快捷键  
我的照片  
我的附件

我的订阅 NEW!  
我的淘宝  
我的空间  
我的相册  
POP3+来信提醒

上一封 | 下一封 | 返回到邮件列表

删除 回复 转发 这是垃圾邮件 移动...

该邮件未标记。[标记邮件 - 标记为未读] 打印页面

From admin@yahoo.cn Mon Apr 21 23:29:17 2008

X-Apparently-To: huangwei@yahoo.cn via 203.209.250.121; Mon, 21 Apr 2008 23:29:17 +0800

X-Originating-IP: [59.64.217.137]

Return-Path: <admin@yahoo.cn>

Authentication-Results: mta101.mail.cnh.yahoo.com from=yahoo.cn; domainkeys=neutral (no sig)

Received: from 59.64.217.137 (EHLO linuxer) (59.64.217.137) by mta101.mail.cnh.yahoo.com with SMTP; Mon, 21 Apr 2008 23:29:17 +0800

Message-ID: <5076660.1208791781448.JavaMail.huangwei@linuxer>

发件人: admin@yahoo.cn 观看联络细节

收件人: huangwei@yahoo.cn

主题: 系统管理员通知

Mime-Version: 1.0

Content-Type: text/plain; charset=GBK

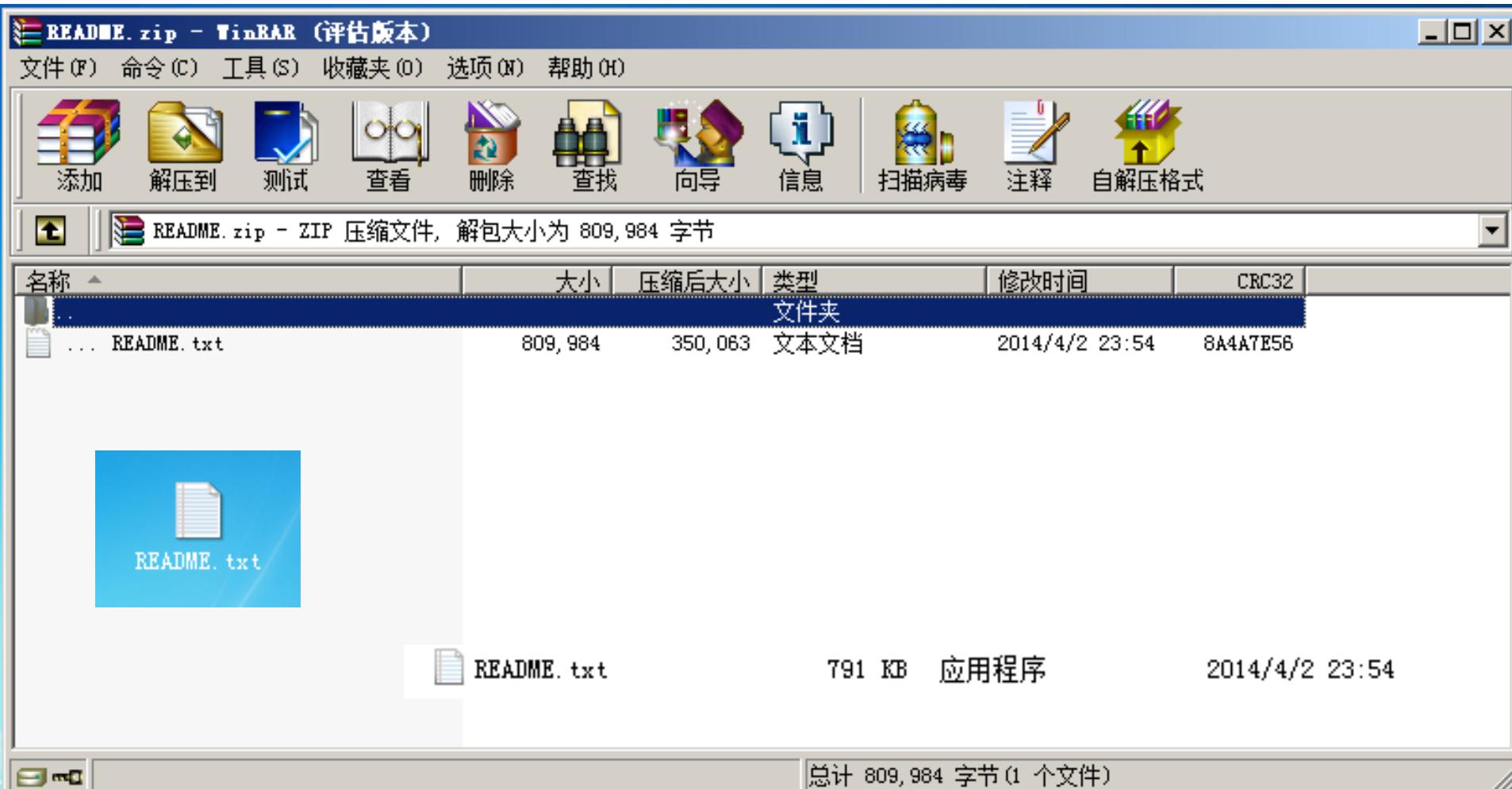
Content-Transfer-Encoding: base64

Content-Length: 9

天哪!



# 社会工程学手段——文件伪装与恶意代码捆绑





## 下载和安装软件



- 国内下载站
- 内部下载站
- 使用XX卫士的软件管家  
——一站式安装
- 卸载不再使用的软件





## 安全软件



- 多多益善
- 病毒库越大越好
- 核心功能必须有
  - 卫士功能
    - 系统和常用软件的安全补丁自动安装功能
    - 系统体检（了解你的电脑的风险等级）
    - 杀毒和卫士功能分离





## 不可忽视的细节(1/3)

- 随手关门
- 门禁卡请保证仅限本人使用
  - 不得借予外人
  - 不得随意借予同事
- 不要在U盘上长期存放公司资料
  - 定期清理和格式化U盘
- 公司保密资料存放
  - 入柜加锁
  - 涉密资料不随身



## 不可忽视的细节(2/3)

- 公开WIFI慎连

- WIFI钓鱼

- 文件共享

- 少用移动存储介质

- 优先选择内网

- FTP

- 飞鸽传书

- 口令共享

- 口传言授不留凭据

LAN口状态

MAC 地址:	40-16-9F-65-A4-D6
IP地址:	192.168.1.1
子网掩码:	255.255.255.0

无线状态

无线功能:	启用
SSID号:	CMCC
信道:	自动 (当前信道 1)
模式:	11bgn mixed
频段带宽:	自动
MAC 地址:	40-16-9F-65-A4-D6
VDS状态:	未开启

WAN口状态



## 不可忽视的细节(3/3)

- 电脑前无人时及时锁屏
- 禁用Windows的文件夹共享功能
  - 关闭Windows的默认共享服务
- 避免在公司电脑上使用外来U盘和移动存储介质
  - 必须使用时务必先杀毒，后打开
- 不在陌生人电脑上输入口令
  - 不确定对方电脑环境的安全程度
- U盘使用完后及时从电脑上拔除



## 参考文献

- ① 微软MBSA <http://technet.microsoft.com/en-us/security/cc184924>
- ② 美国国家漏洞数据库（NVD）的检查清单 <http://web.nvd.nist.gov/view/ncp/repository>
- ③ Ubuntu官方的安全指南 <https://help.ubuntu.com/community/Security>
- ④ SANS Linux Security Checklist (2006.8) [http://www.sans.org\(score/checklists/linuxchecklist.pdf](http://www.sans.org(score/checklists/linuxchecklist.pdf)
- ⑤ wooyun.org <http://www.wooyun.org>
- ⑥ mod\_security参考手册 [http://sourceforge.net/apps/mediawiki/mod-security/index.php?title=Reference\\_Manual](http://sourceforge.net/apps/mediawiki/mod-security/index.php?title=Reference_Manual)



## 课后思考题

- 试举一例说明“人的安全意识和安全能力在应用程序安全加固中是不可忽视的重要环节”