软件安全—恶意代码机理与防护

C1 软件安全概论

彭国军

武汉大学国家网络安全学院

guojpeng@whu.edu.cn

提纲

1.1 信息与信息安全

1.2 软件安全威胁与来源

1.3 软件安全威胁的防护措施

1.1 信息与信息安全

- 以下哪些属于信息？
  - “我是武汉大学的一名教师”
  - 手机收到的天气预报短信：“今天晚上有雨”
  - 网易云平台数据库中存储的用户登录口令
  - 云课堂上的一段MOOC教学视频
  - 课程管理系统中的学生选修名单及成绩
  - 结业证书上的个人与课程信息
  - 期末考试试卷
  - …

1.1.1 什么是信息

- 香农（C.E. shannon）：信息是用来消除随机不确定性的东西
- 其他相关观点：
  - 信息是客体相对于主体的变化。
  - 信息是有价值的消息。
  - 信息是确定性的增加。
  - 信息是反应客观世界中各种事物特征和变化的知识，是数据加工的结果，信息是有用的数据。

信息的表现形式

- 信息可以以多种形式表现：
  - 打印或书写在纸上，
  - 以电子数据的方式存储，
  - 或以胶片形式显示或者通过交谈表达出来等。

信息系统

- 狭义的信息系统：
  - 信息系统(Information System)是以提供信息服务为主要目的的数据密集型、人机交互的计算机应用系统。
- 广义的信息系统≠计算机应用系统

1.1.2什么是安全？

- 安全是指不受威胁，没有危险、不受危害、不受损失的一种可接受状态。
  - 例如：人类与生存环境的和谐相处，互相不伤害，不存在危险的隐患，是免除了不可接受的损害风险的一种状态。
  - 例如：人类生产过程中，将系统的运行状态对人类的生命、财产、环境可能产生的损害控制在人类可接受标准以下的一种状态。

安全（Safety vs Security）

- Safety
  - 自然的，物理的，相对具体的
  - 如房屋、桥梁、大坝…
- Security
  - 社会的，人为的，相对抽象的
  - 如食品、软件…

1.1.3 什么是信息安全？

信息为什么存在安全问题？

信息的主要特点

- **信息是有价值的**
  - 信息的价值是相对的
- 信息是流动的
  - 信源 ---信道-→ 信宿

信息安全的定义

- 对信息的保密性、完整性和可用性的保持。
  - 不可否认性+可控性

C onfidentiality
I ntegrity
A vailability

信息的安全属性

- **保密性：**信息仅被合法用户所知悉。
- **完整性：**数据的一致性，数据未被非法用户篡改。
- **可用性：**合法用户对信息和资源进行使用时，不会被不正当地拒绝。
- **真实性：信息**来源及其内容未被伪造。
- **不可抵赖性：**建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。
- **可审查性：**对出现的信息安全问题提供调查的依据和手段。

信息的价值通过什么来体现？

- 保密性
- 可用性
- 完整性
- 真实性
- 不可否认性
- …

- 网易云平台数据库中存储的用户登录口令
- 期末考试试卷
- 云课堂上的一段MOOC教学视频
- 课程管理系统中的学生选修名单及成绩等

信息的价值在哪些情况下会丧失？

- 泄密（保密性）
- 被盗、损坏（可用性）
- 被篡改（完整性）
- 赖账（不可否认性）
- …

信息安全的实质

- 保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，以维护信息的价值，促进业务的连续性。

- 目前，信息安全已经被提升到了信息保障的地位。

信息保障（Information Assurance）

- 美国国防部对信息保障的定义：
  - “通过确保信息的可用性、完整性、可识别性、保密性和抗抵赖性来保护信息和信息系统，同时引入保护、检测及响应能力，为信息系统提供恢复功能。”

PDRR

=Protection+Detection+Reaction+Restoration

PDR;PPDR;PPDRR

P²DR²

- 信息安全是研究在特定的应用环境下，依据特定的安全策略(Policy)，对信息及其系统实施保护(Protection)、检测(Detection)、响应(Reaction)和恢复(Restoration)的科学。

网络空间安全已经上升为国家安全战略

没有网络安全，就没有国家安全

没有信息化，就没有现代化

- 信息安全事关国家安全、事关社会稳定，信息安全成为国家安全的重要组成部分，必须采取措施确保我国的信息安全。
- 确保我国信息安全，关键是人才。
- 信息安全专业承担着信息安全专业人才培养的重任。

我们是否愿意采取措施来保护我们的信息安全？

- 作为大学生，我们拥有哪些信息？
  - 身份信息
  - 联系方式
  - 社会关系
  - 其他信息：
    - 数码相片/私人信件/口令/电子邮件/聊天记录/好友名单/上网记录/视频聊天/电话清单/协议/保密文件/课程作业/…

我们愿意保护我们的信息吗？

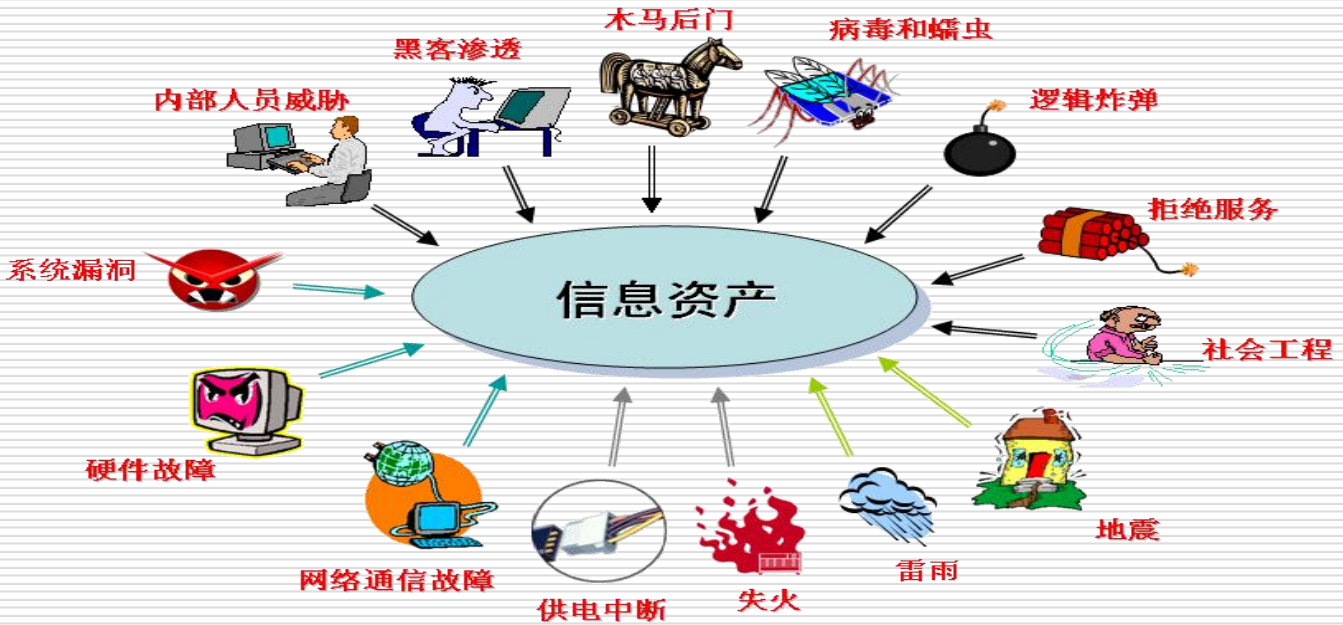
- 该信息的价值有多大？
- 可能面临哪些风险？
- 为保护该信息需要付出多少成本？

  - 在什么情况下愿意采取安全措施？
    - 认识到的价值*认识到的风险>认识到的成本？
  - 是否应该采取安全措施？
    - 真实价值*真实风险>真实成本？

哪些属于软件类威胁？

1.1.4 信息面临哪些安全威胁？

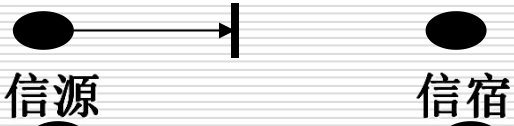
威胁无处不在



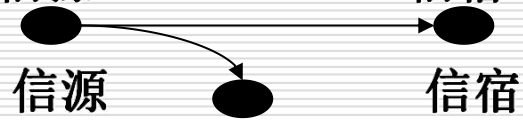
目前的几种攻击模式

正常的信息流动：

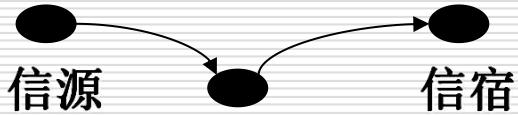
1）中断：



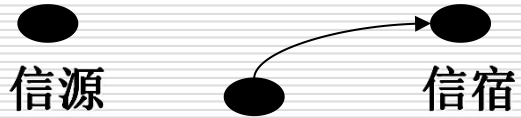
2）截取：



3）修改：

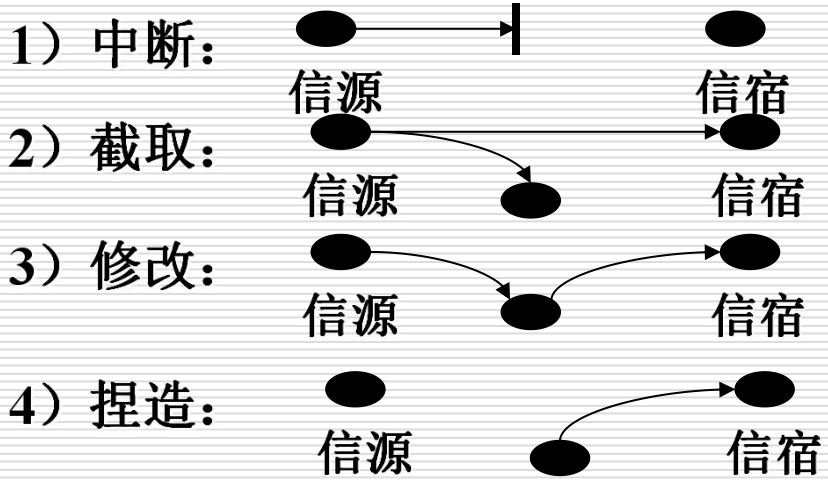


4）捏造：

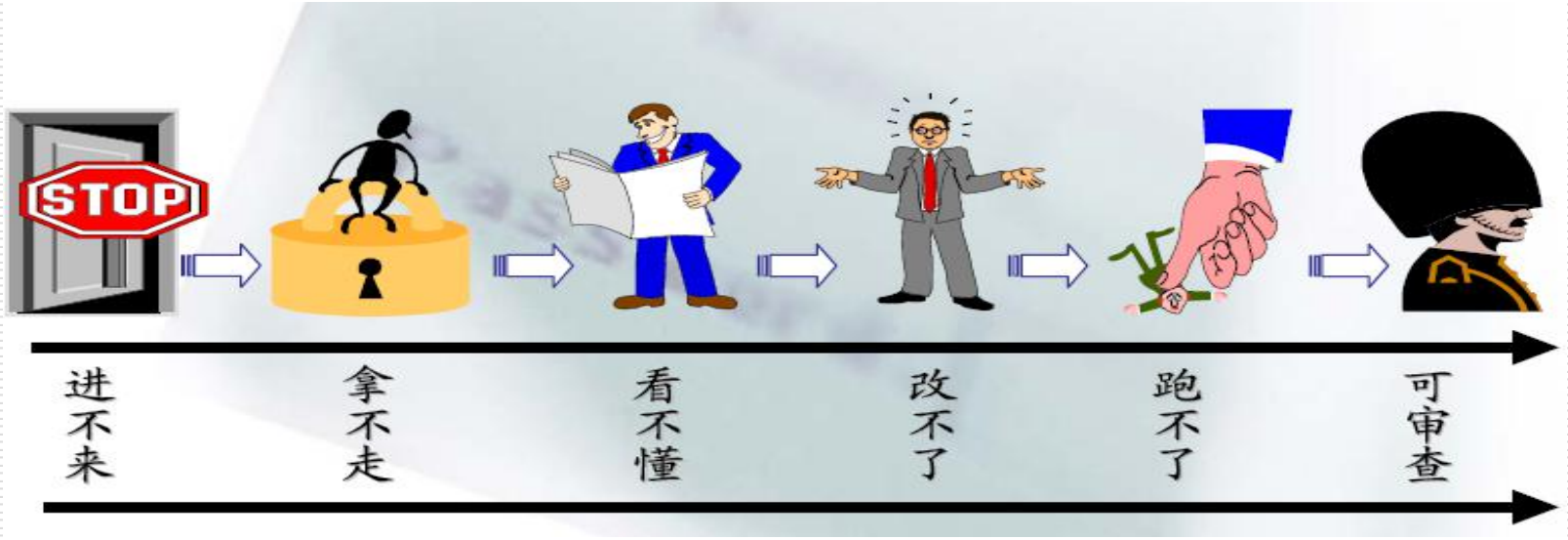


思考

- 以上攻击模式分别破坏了信息的安全属性？



1.1.5 信息安全防护



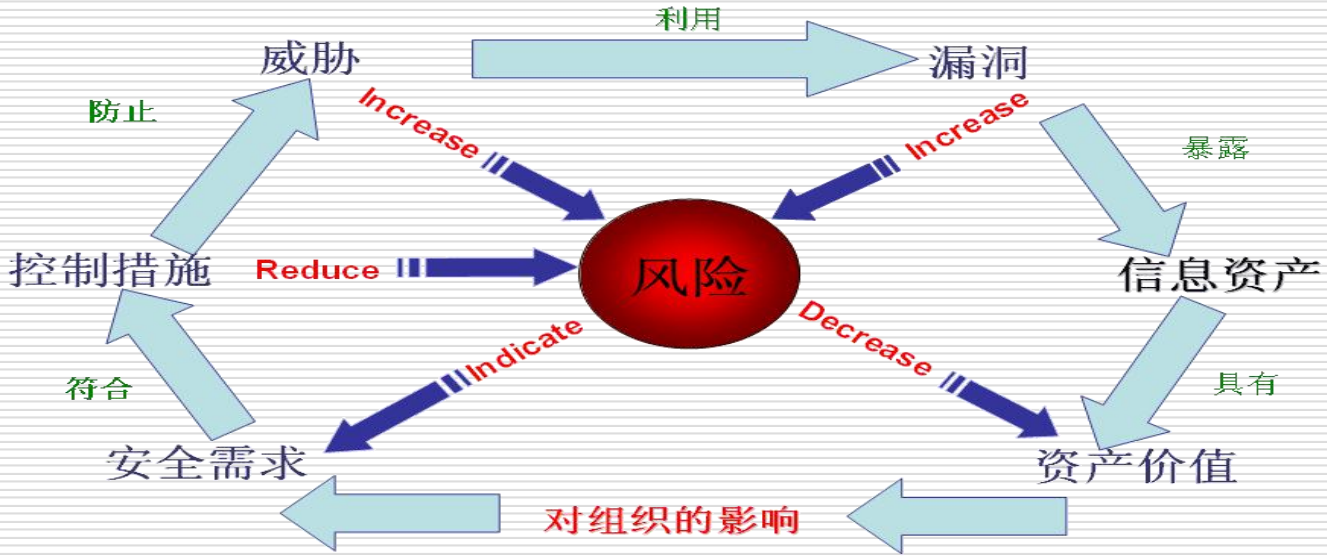
通过什么手段来保障信息安全？

- **安全管理手段**
  - 安全管理制度
  - 安全组织建设
  - 人员安全管理
  - 系统建设管理
  - 系统运维管理等

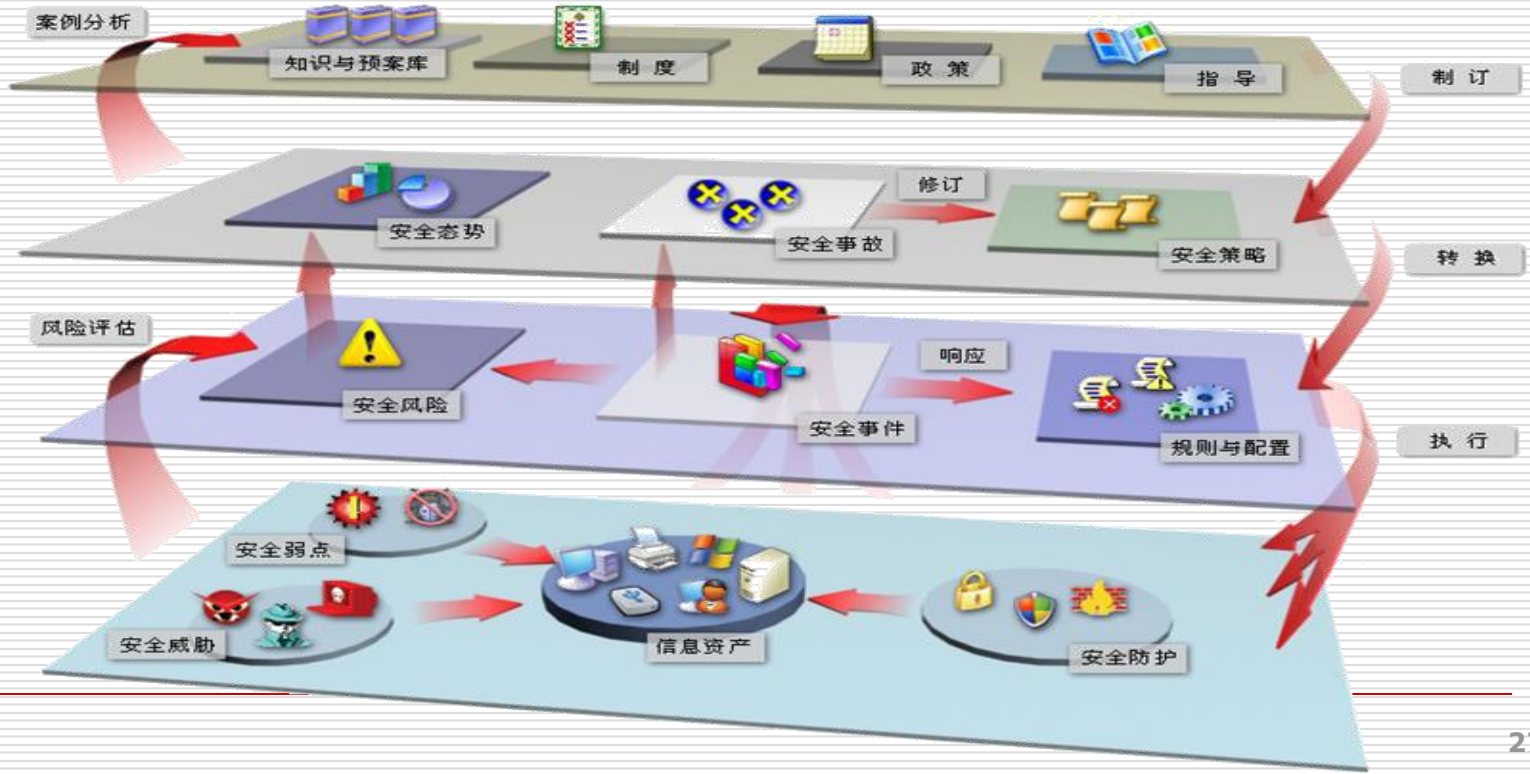
- **安全技术手段**
  - 物理安全、主机安全、网络安全、应用安全、数据安全与备份恢复等
  - 身份认证，访问控制，数据加密，数字签名…
  - 防火墙，杀毒软件…

安全贵在未雨绸缪

因果关系



因果关系（立体）


案例分析
知识与预案库
制 度
政 策
指 导
制 订
安全态势
修订
安全事故
安全策略
转 换
风险评估
安全风险
响应
安全事件
规则与配置
执 行
安全弱点
安全威胁
信息资产
安全防护

1.2 软件安全威胁

- 信息系统面临的三大典型软件安全威胁
  - 软件缺陷与漏洞（正常软件）
  - 恶意软件：实现恶意目的
  - 非法破解，知识产权被侵害（正常软件）

1.2.1 软件缺陷与漏洞

- 软件缺陷（**Defect**），常常又被称作**Bug**
  - 指计算机软件或程序中存在的某种破坏正常运行能力的问题、错误，或者隐藏的功能缺陷。

- 缺陷的存在会导致软件产品在某种程度上不能满足用户的需求。

漏洞

- 漏洞，是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

软件漏洞

- 软件漏洞(Vulnerability)，是指软件在设计、实现、配置策略及使用过程中出现的缺陷，其可能导致攻击者在未授权的情况下访问或破坏系统。

典型软件类型

- 系统软件
  - Windows、Linux、Android、iOS…
- 应用软件
  - MS Office、Acdsee、QQ、迅雷、Acrobat Reader…
- Web软件等
  - 论坛、文章系统、博客…

软件漏洞带来的危害

- 软件正常功能被破坏
- 系统被非法控制和破坏
- 信息泄漏等

微软安全公告— MS14-052

- 最严重的漏洞可能在用户使用 Internet Explorer 查看特制网页时允许远程执行代码。
- 成功利用这些漏洞的攻击者可以获得与当前用户相同的用户权限。那些帐户被配置为拥有较少系统用户权限的客户比具有管理用户权限的客户受到的影响要小。

1 到 15 个公告，共 1211 个　　1　第 1 页，共 81 页

日期	公告号	知识库号	标题	公告等级
2014/9/9	MS14-055	2990928	Microsoft Lync Server 中的漏洞可能允许拒绝服务	重要
2014/9/9	MS14-054	2988948	Windows 任务计划程序中的漏洞可能允许特权提升	重要
2014/9/9	MS14-053	2990931	.NET Framework 中的漏洞可能允许拒绝服务	重要
2014/9/9	MS14-052	2977629	Internet Explorer 的累积性安全更新	严重
2014/8/12	MS14-051	2976627	Internet Explorer 的累积性安全更新	严重
2014/8/12	MS14-050	2977202	Microsoft SharePoint Server 中的漏洞可能允许特权提升	重要
2014/8/12	MS14-049	2962490	Windows Installer 服务中的漏洞可能允许特权提升	重要
2014/8/12	MS14-048	2977201	OneNote 中的漏洞可能允许远程执行代码	重要
2014/8/12	MS14-047	2978668	LRPC 中的漏洞可能允许绕过安全功能	重要
2014/8/12	MS14-046	2984625	.NET Framework 中的漏洞可能允许绕过安全功能	重要
2014/8/12	MS14-045	2984615	内核模式驱动程序中的漏洞可能允许特权提升	重要
2014/8/12	MS14-044	2984340	SQL Server 中的漏洞可能允许特权提升	重要

Microsoft 安全公告 MS14-052 - 严重

此主题尚未评级 - 评价此主题

Internet Explorer 的累积性安全更新 (2977629)

发布日期： 2014 年 9 月 9 日

版本： 1.0

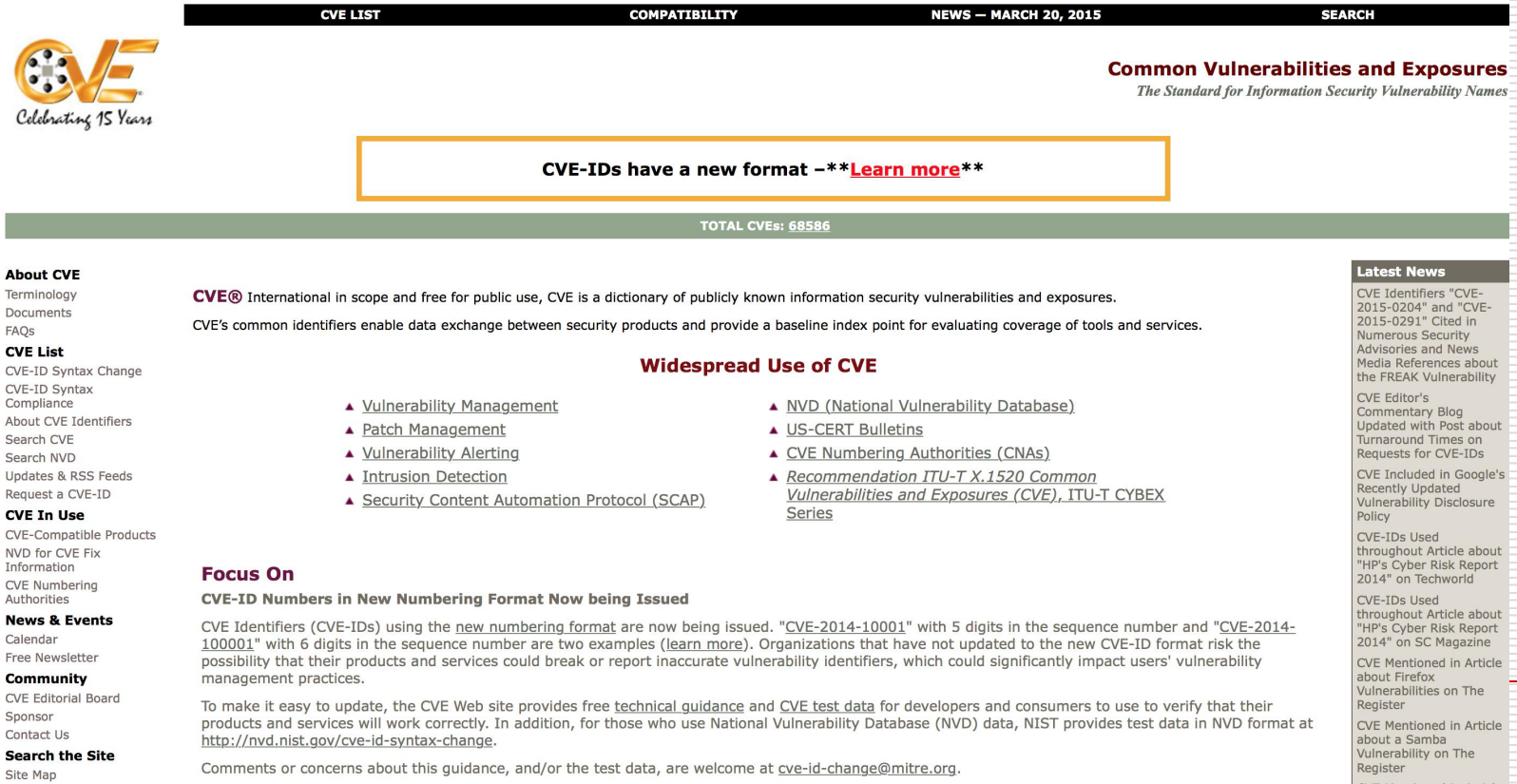
一般信息

摘要

此安全更新可解决 Internet Explorer 中一个公开披露的漏洞和 36 个秘密报告的漏洞。最严重的漏洞可能在用户使用 Internet Explorer 查看特制网页时允许远程执行代码。成功利用这些漏洞的攻击者可以获得与当前用户相同的用户权限。那些帐户被配置为拥有较少系统用户权限的客户比具有管理用户权限的客户受到的影响要小。

对于受影响的 Windows 客户端上的 Internet Explorer 6 (IE 6)、Internet Explorer 7 (IE 7)、Internet Explorer 8 (IE 8)、Internet Explorer 9 (IE 9)、Internet Explorer 10 (IE 10) 和 Internet Explorer 11 (IE 11)，此安全更新的等级为“严重”；对于受影响的 Windows 服务器上的 Internet Explorer 6 (IE 6)、Internet Explorer 7 (IE 7)、Internet Explorer 8 (IE 8)、Internet Explorer 9 (IE 9)、Internet Explorer 10 (IE 10) 和 Internet Explorer 11 (IE 11)，此安全更新的等级为“中等”。有关详细信息，请参阅“**受影响和不受影响的软件**”部分。

CVE—“公共漏洞与暴露”平台



CVE LIST | COMPATIBILITY | NEWS — MARCH 20, 2015 | SEARCH

Celebrating 15 Years

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE-IDs have a new format –Learn more****

TOTAL CVEs: 68586

About CVE
Terminology
Documents
FAQs
CVE List
CVE-ID Syntax Change
CVE-ID Syntax Compliance
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID
CVE In Use
CVE-Compatible Products
NVD for CVE Fix Information
CVE Numbering Authorities
News & Events
Calendar
Free Newsletter
Community
CVE Editorial Board
Sponsor
Contact Us
Search the Site
Site Map

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Use of CVE

- Vulnerability Management
- Patch Management
- Vulnerability Alerting
- Intrusion Detection
- Security Content Automation Protocol (SCAP)
- NVD (National Vulnerability Database)
- US-CERT Bulletins
- CVE Numbering Authorities (CNAs)
- *Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures (CVE)*, ITU-T CYBEX Series

Focus On

CVE-ID Numbers in New Numbering Format Now being Issued

CVE Identifiers (CVE-IDs) using the new numbering format are now being issued. "CVE-2014-10001" with 5 digits in the sequence number and "CVE-2014-100001" with 6 digits in the sequence number are two examples (learn more). Organizations that have not updated to the new CVE-ID format risk the possibility that their products and services could break or report inaccurate vulnerability identifiers, which could significantly impact users' vulnerability management practices.

To make it easy to update, the CVE Web site provides free technical guidance and CVE test data for developers and consumers to use to verify that their products and services will work correctly. In addition, for those who use National Vulnerability Database (NVD) data, NIST provides test data in NVD format at http://nvd.nist.gov/cve-id-syntax-change.

Comments or concerns about this guidance, and/or the test data, are welcome at cve-id-change@mitre.org.

Latest News

CVE Identifiers "CVE-2015-0204" and "CVE-2015-0291" Cited in Numerous Security Advisories and News Media References about the FREAK Vulnerability

CVE Editor's Commentary Blog Updated with Post about Turnaround Times on Requests for CVE-IDs

CVE Included in Google's Recently Updated Vulnerability Disclosure Policy

CVE-IDs Used throughout Article about "HP's Cyber Risk Report 2014" on Techworld

CVE-IDs Used throughout Article about "HP's Cyber Risk Report 2014" on SC Magazine

CVE Mentioned in Article about Firefox Vulnerabilities on The Register

CVE Mentioned in Article about a Samba Vulnerability on The Register

CNVD & CNNVD


登录 免费注册
CNVD
国家信息安全漏洞共享平台
CHINA NATIONAL VULNERABILITY DATABASE
首页
热点关注
漏洞列表
补丁信息
安全公告
统计查询
研究报告
工作体系
统计数据
高级搜索
成员单位工作贡献排名（2015-03-16 - 2
1,000
900
800
700
600
500
400
300
200
100
0
奇虎360
天融信
启明星辰
安天
恒安嘉新
北京神州绿盟科技
漏洞查询
证书查询
漏洞报送
漏洞跟踪
热点推荐
热点新闻
> More
关于GNU glibc函数库存在缓冲区溢出高危漏洞（“幽灵”漏洞）的情况公告 2015-01-29
微软披露影响所有Windows版本的高危漏洞 2014-11-18
关于GNU Bash存在远程代码执行漏洞的情况通报 2014-09-26
关于Internet Explorer VGX.DLL远程代码执行漏洞的安全公告 2014-04-28
关于Apache Struts 2存在补丁绕过漏洞的情况公告 2014-04-24
关于OpenSSL存在高危漏洞可被利用发起大规模攻击的情况通报（4月9日结果） 2014-04-09
上周最受关注漏洞
漏洞标题 点击数
1 phpMoAdmin任意命令执... [1286]
2 724CMS SQL 'ID'参数S... [1226]
3 IBM API Management信... [1226]
4 Apache mod-gnutls证书... [1208]
5 automount权限提升漏洞... [1201]
漏洞信息
补丁信息
> More
漏洞名称 点击数 时间
多个产品SMM本地代码执行漏洞 29 2015-03-27
漏洞趋势
周 月 年
2015-03-16 - 2015-03-22
50
45


中国国家信息安全漏洞库
China National Vulnerability Database of Information Security
首页
漏洞信息
补丁信息
业界新闻
漏洞提交
查询统计
分析报告
常见问题
合作伙伴
CNNVD 服务
基本服务
CNNVD漏洞基本通报服务，主要为用户提供漏洞信息基本通报服务（含Top5最受关注漏洞及信息安全漏洞月报）及与CNNVD相关...进入服务
1 2 3
业界新闻 更多..
利用Instagram API制 ... 03/27
黑客利用PDF生成 ... 03/27
SELinux防御被轻易 ... 03/27
朝鲜否认与韩国 ... 03/27
12306图片验证码被 ... 03/27
黑客可通过电脑 ... 03/27
分析报告 更多..
信息安全漏洞月通报(2015年2月)
信息安全漏洞月通报(2015年1月)
信息安全漏洞月通报(2014年12月)
信息安全漏洞月通报(2014年11月)
信息安全漏洞月通报(2014年10月)
信息安全漏洞月通报(2014年9月)
网站简介 更多..
中国国家信息安全漏洞库，英文名称"China National Vulnerability Database
最受关注漏洞
1 厂商：X.Org 发布日期：2015-03-23
漏洞名称：X.Org libXfont 安全漏洞
漏洞编号：CNNVD-201503-409
补丁
2 厂商：OpenSSL 发布日期：2015-03-20
漏洞名称：OpenSSL'EVP_DecodeUpdate'函数整 ...
漏洞编号：CNNVD-201503-404
补丁
3 厂商：IBM 发布日期：2015-03-19
漏洞名称：IBM Rational DOORS Next Generation和 ...
漏洞编号：CNNVD-201503-357
补丁
4 厂商：Adobe 发布日期：2015-03-16
漏洞名称：Adobe Flash Player 资源管理错误 ...
漏洞编号：CNNVD-201503-321
补丁
5 厂商：Cisco 发布日期：2015-03-16
漏洞名称：多款Cisco产品授权问题漏洞
漏洞编号：CNNVD-201503-308
补丁
其他漏洞信息 更多..
CNNVD-201503-588 WebGate eDVR Manager ActiveX C ... 2015-03-27
CNNVD-201503-587 Websense TRITON AP-WEB 安全漏 ... 2015-03-27
CNNVD-201503-586 Websense TRITON和V-Series 跨 ... 2015-03-27
CNNVD-201503-585 Websense TRITON和V-Series 安 ... 2015-03-27
CNNVD-201503-584 Citrix Systems Command Center ... 2015-03-27
CNNVD-201503-583 Citrix Systems Command Center ... 2015-03-27
CNNVD-201503-582 Red Hat JBoss RichFaces 安全 ... 2015-03-27
CNNVD-201503-581 Cisco Mobility Services Engine ... 2015-03-27
CNNVD-201503-580 Cisco IOS XR DHCPv4服务器拒 ... 2015-03-27
CNNVD-201503-579 Cisco IOS和IOS XE Service Dis ... 2015-03-27
漏洞提交
漏洞提交须知
提交漏洞
站内搜索
请输入相关关键字
搜 索
补丁信息 更多..
1. CNPD-201503-0261 openssl-1.0.2a
2. CNPD-201503-0260 openssl-1.0.1m
3. CNPD-201503-0259 openssl-1.0.0r
4. CNPD-201503-0258 openssl-0.9.8zf
5. CNPD-201503-0253 openssl-1.0.2a
6. CNPD-201503-0247 requests_2.3.0-1ubuntu0. ...
Flash 已过期

乌云漏洞公布平台

登录 | 注册

WooYun.org 加关注 13.2万

首页 | 厂商列表 | 白帽子 | 乌云榜 | 团队 | 漏洞列表 | 提交漏洞 | 安全中心 | 乌云招聘 | 知识库 | 公告

当前位置：WooYun >> 首页

WooYun支持在等级不够时使用乌云币提前查看漏洞

最新提交 (58)

提交日期	漏洞名称	评论/关注	作者
2015-03-28	国家超级计算某中心某系统漏洞可导致内网漫游(点到为止)	17/39	管管侠
2015-03-28	一起飞一个弱口令引发的血案	0/1	路人甲
2015-03-28	易车某核心业务存在时间注入	0/0	Comer
2015-03-28	网站安全狗免杀神技+IIS6.0解析WebShell访问限制Bypass	2/18	RedFre...
2015-03-28	边锋网络某处SQL注入	0/1	路人甲
2015-03-28	Wecenter最新版注入之二（黑盒测试技巧）	2/19	Xser

最新确认 (1124)

提交日期	漏洞名称	评论/关注	作者
2015-03-28	美丽说另一站点MySQL盲注	0/1	lijiej...
2015-03-28	美丽说某站点MySQL报错注入(用户数据15万)	0/2	lijiej...
2015-03-28	和讯财经APP接口注射	2/6	greg.w...
2015-03-25	机锋网某dubbo未授权访问	0/10	路人甲
2015-03-28	拉手网部分商户信息泄露	0/2	咸鱼翻...
2015-03-28	拉手团购某分站存在post注入	0/3	路人甲

WooYun-2013-34935：
如家等大量酒店客户开房记录被第三方存储并因漏洞导致泄露

WooYun.org 加关注 13.2万

首页 | 厂商列表 | 白帽子 | 乌云榜 | 团队 | 漏洞列表 | 提交漏洞 | 安全中心 | 乌云招聘 | 知识库 | 公告

当前位置：WooYun >> 漏洞信息

漏洞概要

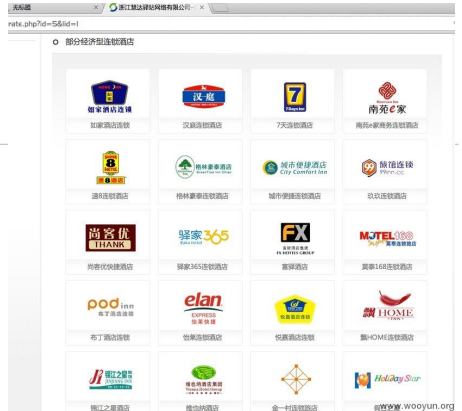
关注数(67) 关注此漏洞

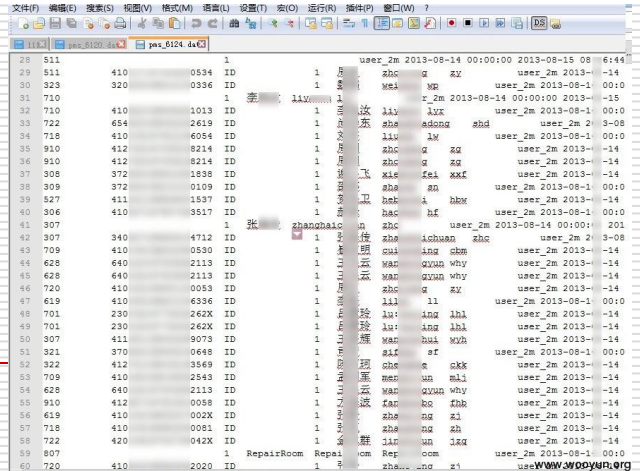
缺陷编号： **WooYun-2013-34935**
漏洞标题： 如家等大量酒店客户开房记录被第三方存储并因漏洞导致泄露
相关厂商： **浙江慧达驿站网络有限公司**
漏洞作者： **Yep**
提交时间： 2013-08-21 23:21
公开时间： 2013-10-05 23:22
漏洞类型： 敏感信息泄露
危害等级： 高
自评Rank： 10
漏洞状态： 已交由第三方合作机构(cncert国家互联网应急中心)处理
漏洞来源： **http://www.wooyun.org**
Tags标签： 敏感信息泄露 用户敏感信息泄露
分享漏洞： 分享到

漏洞详情

披露状态：

2013-08-21： 细节已通知厂商并且等待厂商处理中
2013-08-26： 厂商已经确认，细节仅向厂商公开
2013-09-05： 细节向核心白帽子及相关领域专家公开
2013-09-15： 细节向普通白帽子公开
2013-09-25： 细节向实习白帽子公开
2013-10-05： 细节向公众公开





1.2.2 恶意软件

- “恶意软件”是指那些设计目的是为了实施特定恶意功能的一类软件程序。

- 典型的恶意软件种类：
  - 计算机病毒、蠕虫、特洛伊木马、后门、僵尸、间谍软件等。

恶意软件威胁

- 修改或破坏已有软件的功能
  - 恶意软件运行之后，可以对同一运行环境中的其他软件进行干扰和破坏，从而修改或者破坏其他软件的行为。
- 窃取目标系统中的重要数据
  - 数据库、文档、口令等（灰鸽子、上兴、Flame）
- 监视目标系统中的用户行为
  - 对目标系统进行屏幕监视、视频监视、语音监听等
- 控制目标系统等
  - Shell、屏幕控制、跳板等

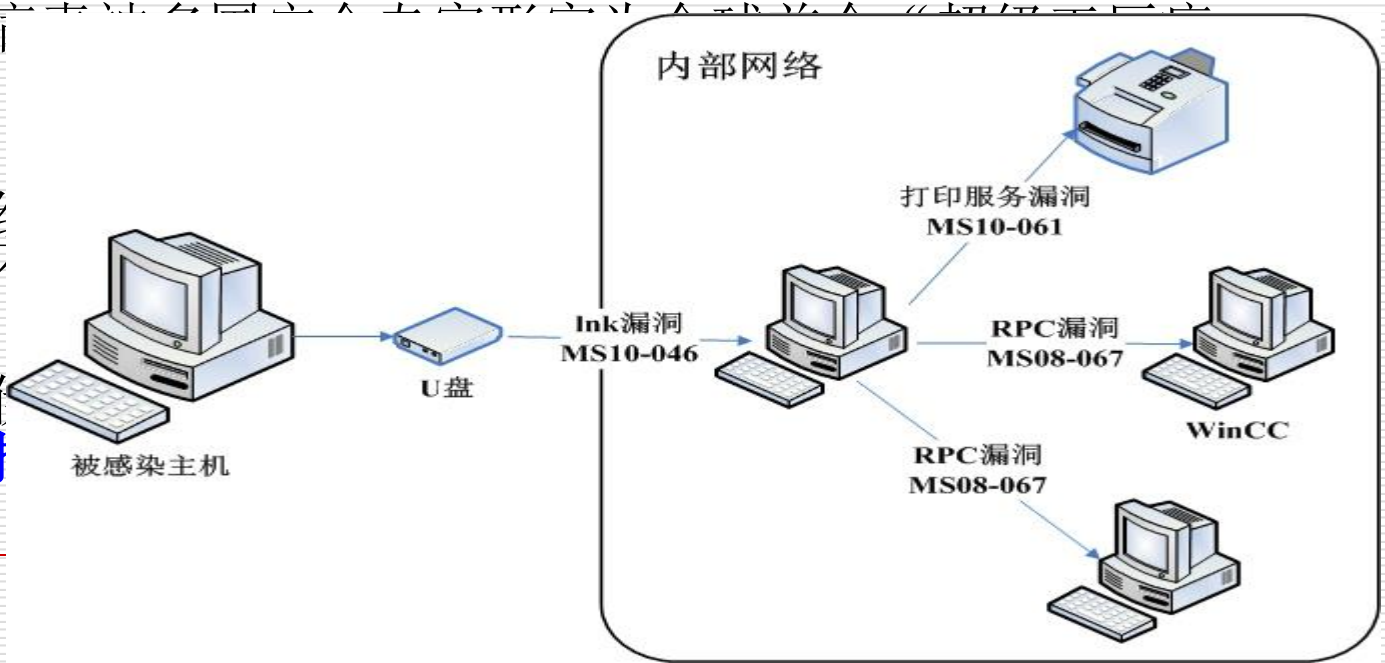
功能被破坏：武汉千余出租车计价失灵

- 2008年8月8日凌晨0时许，武汉市千余辆的士的计价器突然死机，导致人车停岗四小时。

浙江在线08月22日讯 8月8日凌晨零点起，杭城约有1100辆出租车计价器发生病毒感染，集体失灵。次日，等候维修的出租车陆续聚集在杭州市质量技术监督检测院外，形成了近3公里的“长龙”。这一天不仅仅是杭州的出租车计价器出了问题，武汉、厦门等地的出租车也遇到了这样的尴尬。这次出租车集体中毒事件让不少当天准备打的出行的市民受到影响，并且引起了人们广泛的关注。

Stuxnet(超级工厂病毒)：破坏伊朗核电站铀浓缩装置

- 2010年7月大面积爆发。
- Stuxnet病毒被多国安全专家形容为全球首个“超级工厂病毒”。
- 该病毒已经[illegible]等多地均[illegible]
- 其中，以伊[illegible]尔核电站[illegible]



付款被劫持

楚天都市报

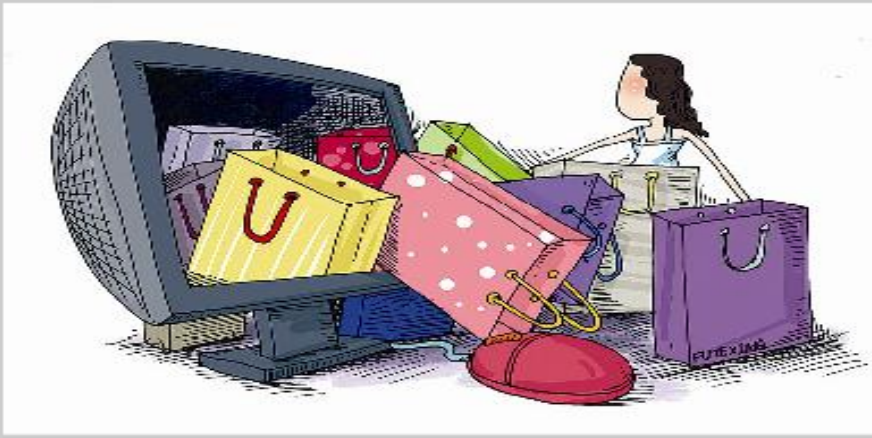
2010年9月13日 星期一

返回首版 | 版面导航 | 标题导航 | 最小化 | 退出

日期检索： 文章搜索

2 2010/09/13 网购黑客陷阱调查·案例

图文：网购货款被黑客劫至陌生账户



本报记者王昱晔 张泉 见习记者夏宇 统筹：记者杨向明

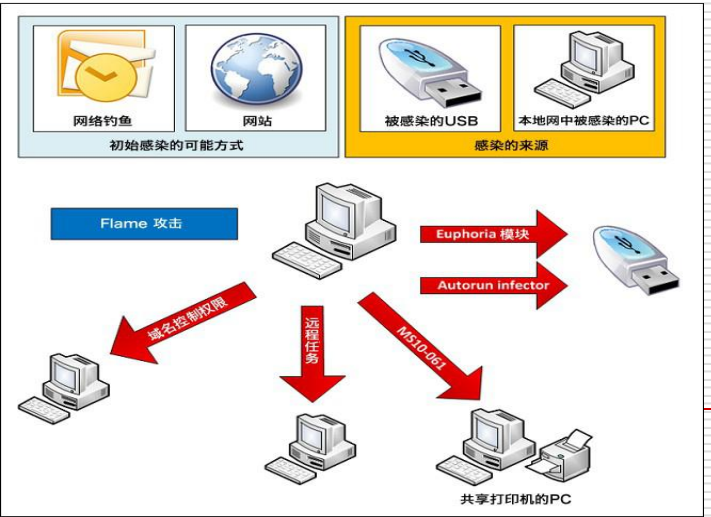
网上购物因其便捷、实惠、安全，已成为人们特别是年轻一代的生活方式之一。然而，武昌顾先生的亲身经历则提醒大家，网购在安全性方面亦可能存在漏洞。

机密数据泄漏

- 中国机密遭境外网络间谍围攻（攻击、策反和传输）：
  - 中原某军工科研所彭某：**国防科工委办公厅的中秋贺卡**（参与中国海军潜艇科研项目的大量军工科研项目的资料泄露）
  - 湖南某大学孙某（参与北方某军工院校重要军工项目）：**国际学术会议的电子邀请函**（重要军事武器项目资料泄露）
  - 能源化工某领域西南地区学术带头人周某：**朋友的电子贺卡**（涉及22个省的多个重大能源化工项目资料泄露）

Flame（火焰）

5 种加密算法，3 种压缩技术，至少 5 种文件格式，65万行代码，编写复杂。卡巴斯基实验室表示，要全面了解Flame病毒，可能得花上10年时间。



“网络重武器”火焰病毒攻击伊朗能源设施

发布时间:2012-5-30 13:39:09

俄罗斯电脑病毒防控机构卡巴斯基

Flame病毒体积较大 全面了解需10年

来源：腾讯科技　编辑：userz　发布时间：2012-05-29 15:34　浏览：　发表评论

北京时间5月29日消息，据国外媒体报道，俄罗斯**反病毒公司**卡巴斯基实验室(以下简称“卡巴斯基”)近日表示，一种名为“Flame”的恶意间谍软件已在中东和北非部分地区得以大范围传播，该病毒已经或即将造成的巨大危害不可忽视。

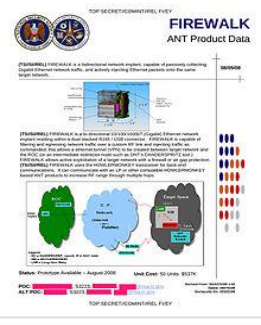
该病毒由卡巴斯基首先发现，并根据该病毒内部代码所含字样，而将其命名为“Flame”。卡巴斯基称，Flame实际上是一个间谍工具包。至少过去两年中，Flame病毒已感染了伊朗、黎巴嫩、叙利亚、苏丹、其他中东和北非国家的相应目标计算机系统。

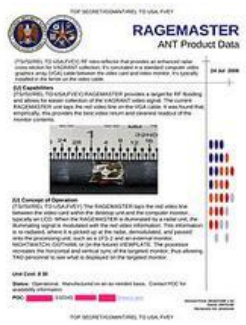
破坏＋窃取

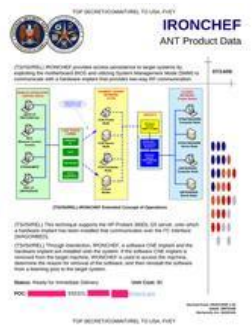
- 三大恶意软件攻击目标互补：
  - Stuxnet ：破坏伊朗核设施（2010年被发现，4个系统漏洞，＋2个WinCC漏洞）
  - Duqu：窃取伊朗工业控制系统数据（2011年被发现）
  - Flame：窃取伊朗石油部门的商业情报。（2012年5月被卡巴斯基发现，部署于至少4年以前）

国家背景的攻击行为日益突显，实力雄厚，组织性强

- NSA监听军火库—ANT：
  - 在全球网络中为情报部门开启“后门”，并植入间谍软件
  - 从计算中心到个人电脑，从笔记本到手机无一能够幸免







1.2.3 软件破解

- 软件破解，即通过对软件自身程序进行逆向分析，剖析软件的注册机制，对软件的各类限制实施破解，从而使得非法使用者可以正常使用软件。

- 软件破解是对软件版权和安全的一个重大挑战。

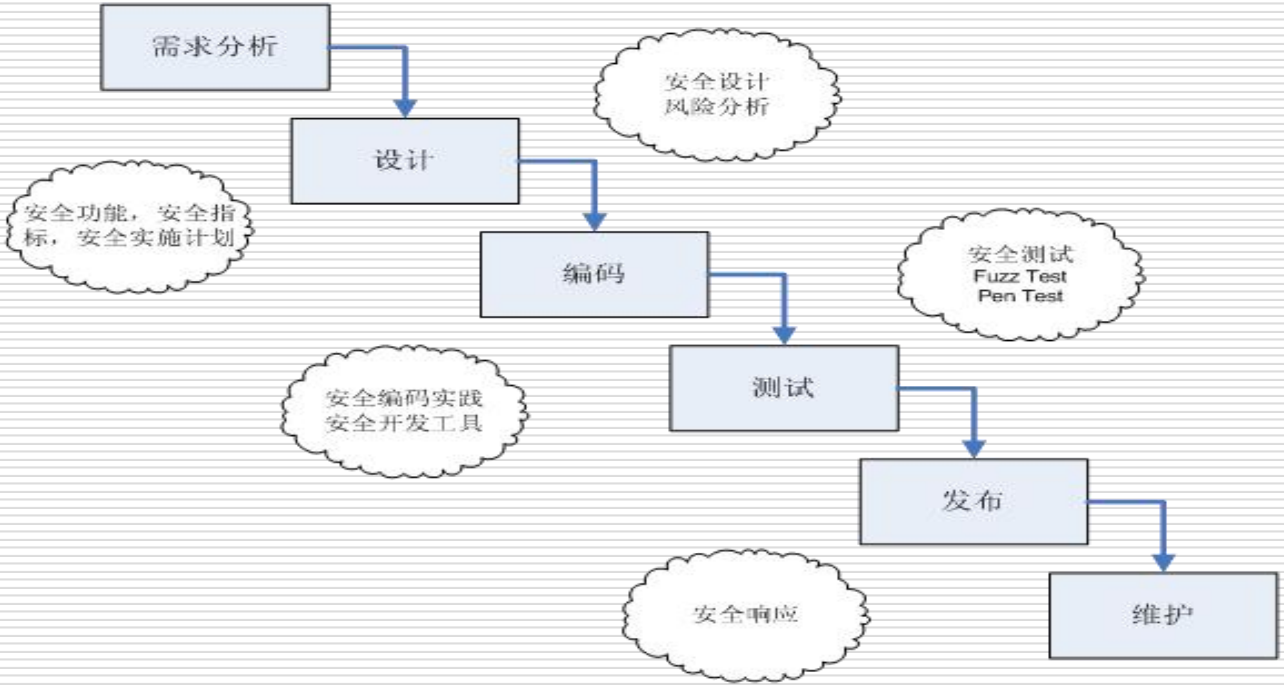
1.3 软件安全防护手段

- 安全设计
- 保障运行环境
- 加强软件自身行为认证
- 恶意软件检测与查杀
- 黑客攻击防护
- 系统还原
- 虚拟隔离等。

1.3.1 安全设计

- 强化软件工程思想，将安全问题融入到软件的开发管理流程之中，在软件开发阶段尽量减少软件缺陷和漏洞的数量。
- 微软：信息技术安全开发生命周期流程 （Secure Development Lifecycle for Information Technology，缩写为SDL-IT）。
  - 该流程包含有一系列的最佳实践和工具，用于微软内部业务应用以及许多微软客户的开发项目中。
  - 微软的Windows 7、8系统

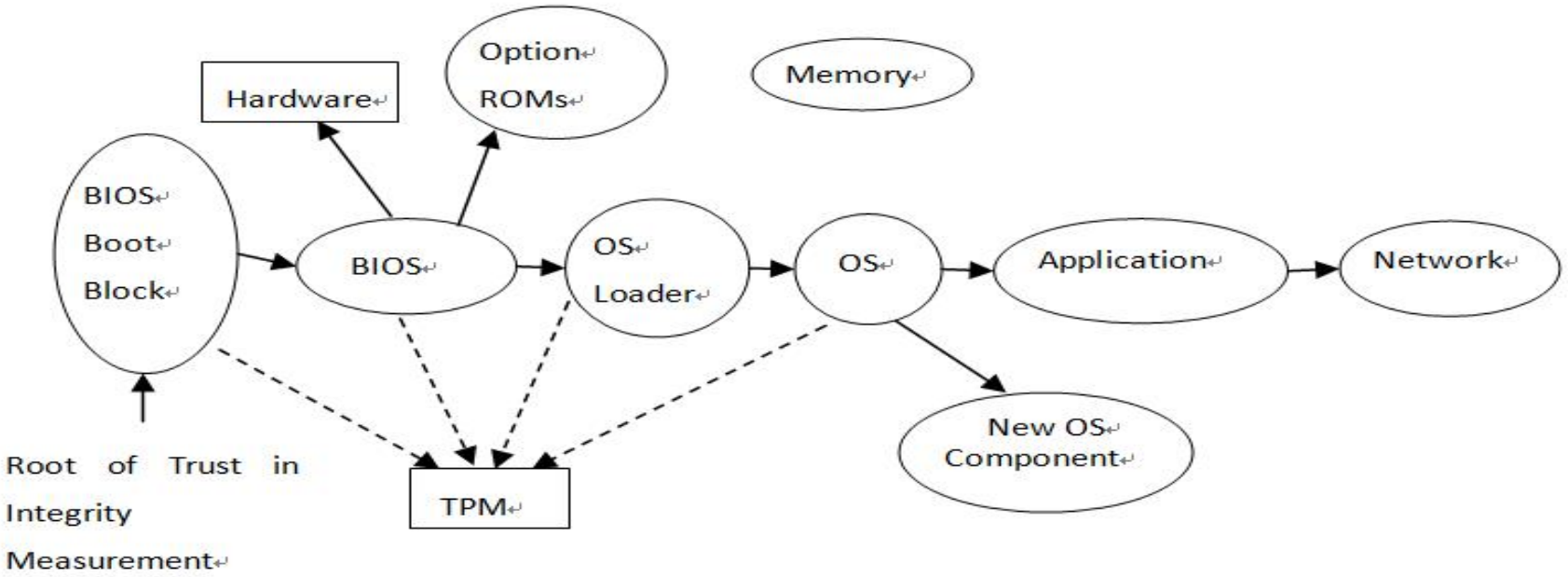
SDL开发模式


需求分析
设计
编码
测试
发布
维护
安全设计
风险分析
安全功能，安全指标，安全实施计划
安全测试
Fuzz Test
Pen Test
安全编码实践
安全开发工具
安全响应

1.3.2 保障运行环境

- 保障软件自身运行环境，加强系统自身的数据完整性校验
  - 软件完整性校验
    - 目前很多安全软件在安装之初将对系统的重要文件进行完整性校验并保存其校验值， 如卡巴斯基安全套件。
  - 系统完整性校验
    - 目前有些硬件系统从底层开始保障系统的完整性，可信计算思想是典型代表。

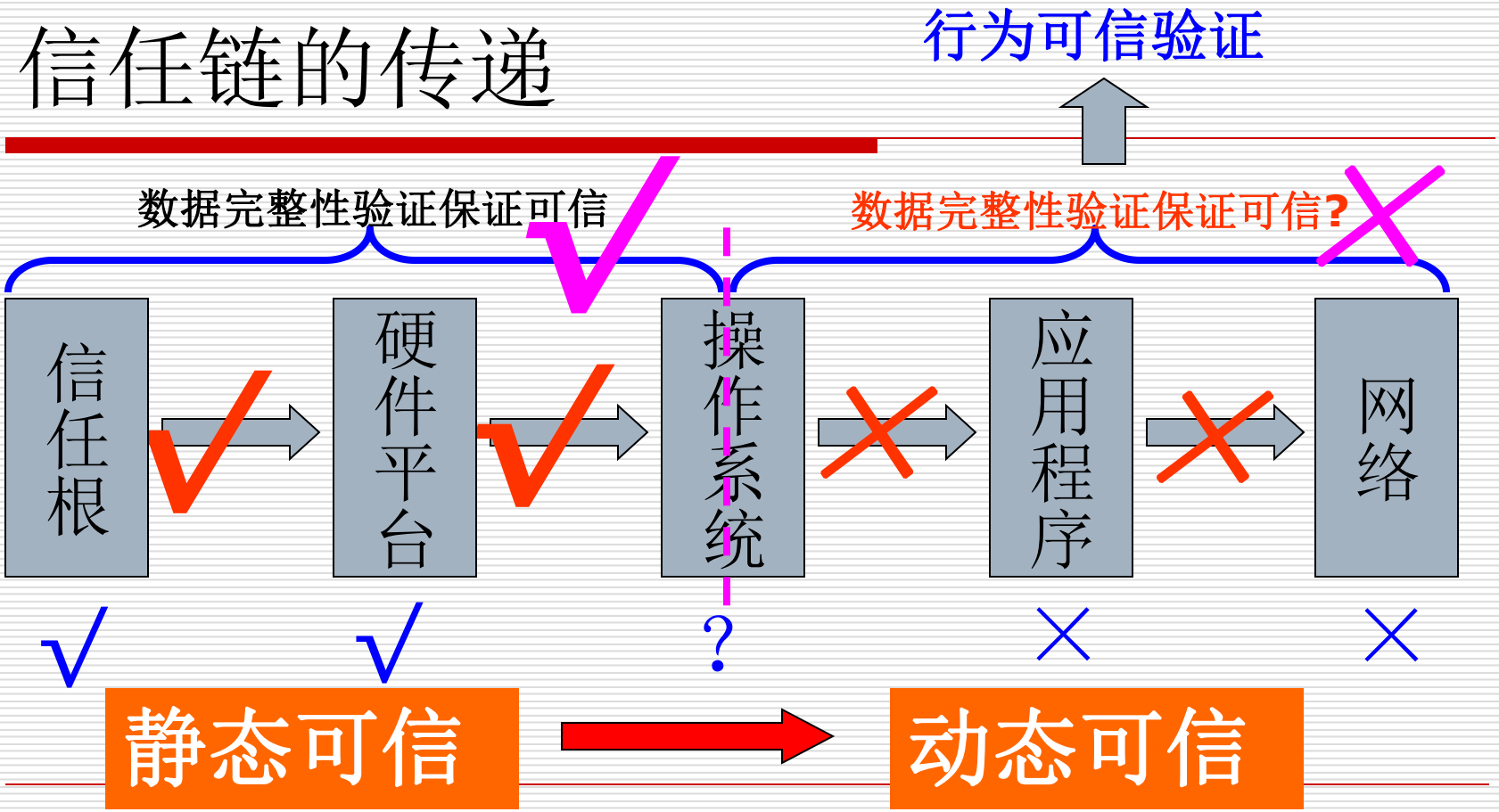
TCG的可信计算信任链的传递



1.3.3 加强软件自身行为认证

- 软件动态可信认证
  - 在确保软件数据完整性的前提下，如何确保软件的行为总是以预期的方式，朝着预期的目标运行。

信任链的传递


行为可信验证
数据完整性验证保证可信
数据完整性验证保证可信?
信任根
硬件平台
操作系统
应用程序
网络
?
静态可信
动态可信

高可信软件技术研究

- **美国计算研究协会:**把高可信软件系统看作是目前计算机研究领域必须应对的五大挑战之一。
- **美国国家科技委员会:**在其总统财政预算报告中指出，高可信软件技术是需要优先开展的研究工作，包括构造更加安全、可靠和健壮的可信软硬件平台，提供更高效的可信软件开发技术，以及建立新的保证复杂软件系统高可信的科学和工程体系等。
- **美国国防部高级研究计划署（Defense Advanced Research Projects Agency，DARPA）:**将高可信系统和软件列为目前需要面对的四大挑战之一。
- **美国国家科学基金会、美国宇航局和美国安全局（National Security Agency，NSA）等:**高可信软件技术研究的重要投资方。
- **微软：**可信赖计算(Trustworthy computing,TWC)

- 我国政府十分重视软件系统的可信性问题。
  - 国家自然科学基金委从2007年启动了“可信软件基础研究”重大研究计划；
  - 国家高技术发展（863）计划中设立了专门的重大项目，研究高可信软件生产工具及集成环境；
  - 国家重点基础研究发展（973）计划将可信软件的研究确定为重点发展方向，研究基于网络的复杂软件可信度和服务质量。

- 为了集中技术力量进行专项研究，我国还设置了可信软件的专项实验室
  - **华东师范大学：**高可信软件技术教育部重点实验室和上海市高可信计算重点实验室等。
  - **武汉大学：**“空天信息安全与可信计算”教育部重点实验室。

1.3.4 恶意软件检测与查杀

- 反病毒软件主要用来对外来的恶意软件进行检测。
  - 通常采用病毒特征值检测、虚拟机、启发式扫描、主动防御、云查杀等等几种方法来对病毒进行检测。

- 恶意软件是软件安全的一个主要安全威胁来源，针对系统的外来入侵通常都离不开外来恶意软件的支撑。

1.3.5 黑客攻击防护

- 防火墙
  - 网络、主机防火墙
- 入侵检测系统IDS
- 入侵防护系统IPS
  - 基于网络、基于主机（HIPS）
- 基于主机的漏洞攻击阻断技术
  - EMET：Microsoft's Enhanced Mitigation Experience Toolkit

1.3.6 系统还原

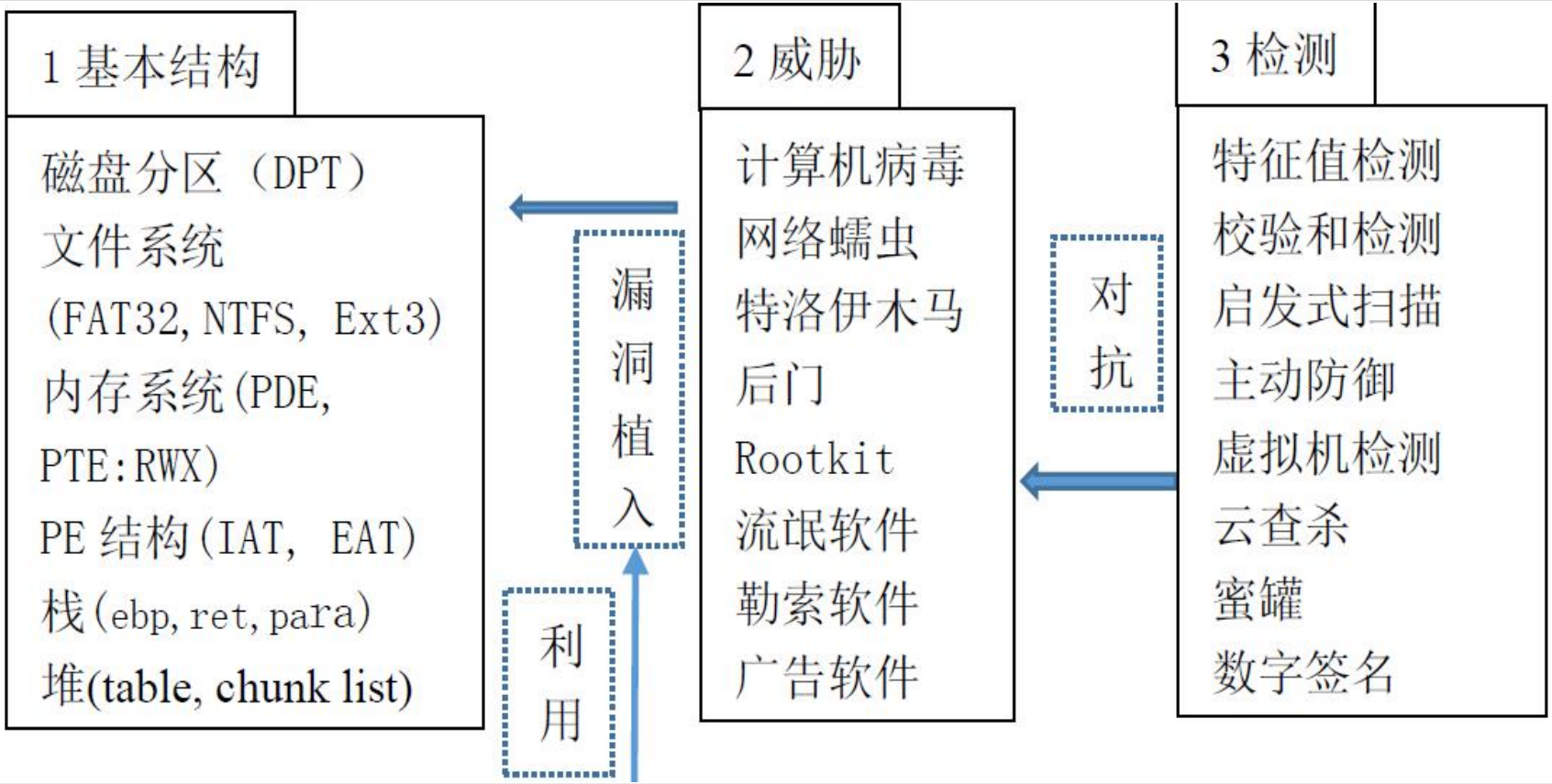
- 将关键系统文件或指定磁盘分区还原为之前的备份状态，从而将已有系统中的恶意程序全部清除，以保护系统安全。
  - Windows自带的“系统还原”功能
  - Ghost还原软件
  - 还原卡、影子系统（PowerShadow）等

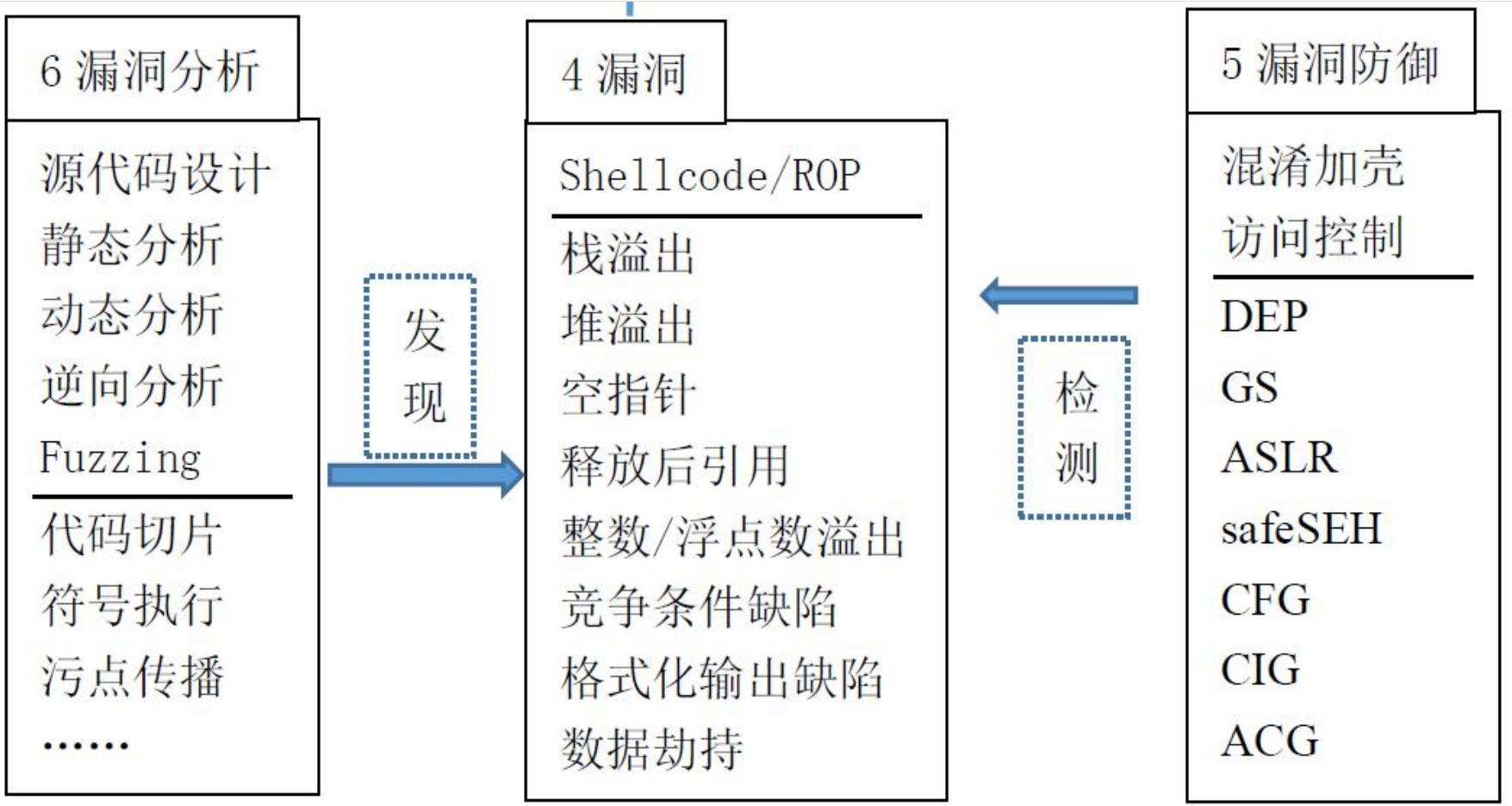
1.3.7 虚拟隔离等

- 虚拟机（如VmWare）
  - 隔离风险
    - 用户可以通过在不同的虚拟机中分别进行相关活动（如上网浏览、游戏或网银等重要系统登陆），从而可以将危险行为隔离在不同的系统范围之内，保障敏感行为操作的安全性。
- 沙箱，也叫沙盘或沙盒（如SandBoxIE）
  - 隔离风险
  - 通常用于运行一些疑似危险样本，从而可以隔离安全威胁，也可以用于恶意软件分析。

课后思考

- 什么是我们身边的信息安全？
- Safety与Security的区别是什么？
- 信息系统存在安全问题的本质原因是什么？
- 信息安全问题为何日益严重？
- 软件安全防护手段有哪些？它们各自从哪些角度来保障信息安全？


1 基本结构
磁盘分区（DPT）
文件系统
(FAT32, NTFS, Ext3)
内存系统(PDE,
PTE:RWX)
PE 结构(IAT, EAT)
栈(ebp, ret, para)
堆(table, chunk list)
漏洞植入
利用
2 威胁
计算机病毒
网络蠕虫
特洛伊木马
后门
Rootkit
流氓软件
勒索软件
广告软件
对抗
3 检测
特征值检测
校验和检测
启发式扫描
主动防御
虚拟机检测
云查杀
蜜罐
数字签名


6 漏洞分析
源代码设计
静态分析
动态分析
逆向分析
Fuzzing
代码切片
符号执行
污点传播
……
发现
4 漏洞
Shellcode/ROP
栈溢出
堆溢出
空指针
释放后引用
整数/浮点数溢出
竞争条件缺陷
格式化输出缺陷
数据劫持
检测
5 漏洞防御
混淆加壳
访问控制
DEP
GS
ASLR
safeSEH
CFG
CIG
ACG

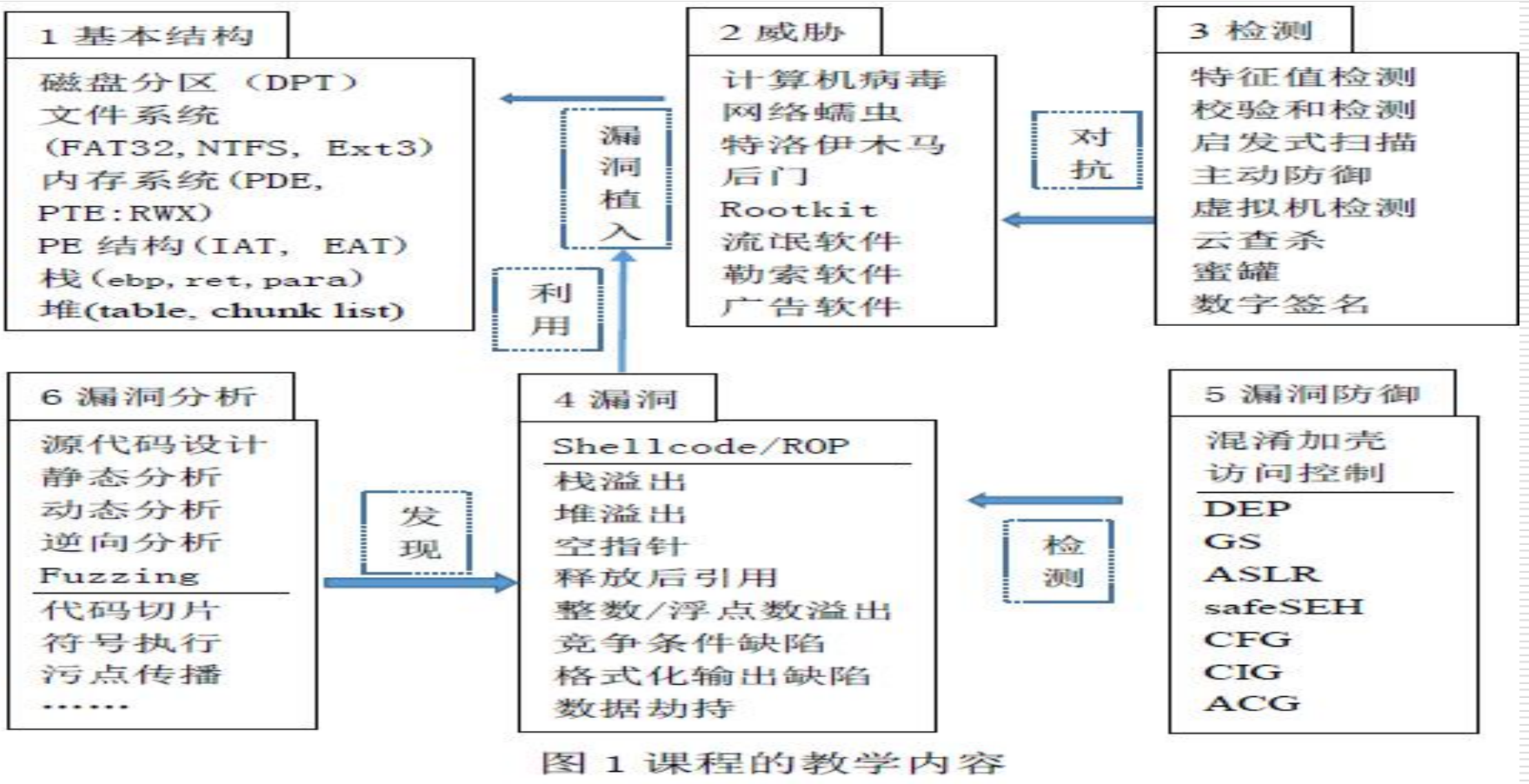

1 基本结构
磁盘分区（DPT）
文件系统
（FAT32, NTFS, Ext3）
内存系统（PDE,
PTE:RWX）
PE 结构（IAT, EAT）
栈（ebp, ret, para）
堆(table, chunk list)
2 威胁
计算机病毒
网络蠕虫
特洛伊木马
后门
Rootkit
流氓软件
勒索软件
广告软件
3 检测
特征值检测
校验和检测
启发式扫描
主动防御
虚拟机检测
云查杀
蜜罐
数字签名
漏洞植入
对抗
利用
6 漏洞分析
源代码设计
静态分析
动态分析
逆向分析
Fuzzing
代码切片
符号执行
污点传播
……
发现
4 漏洞
Shellcode/ROP
栈溢出
堆溢出
空指针
释放后引用
整数/浮点数溢出
竞争条件缺陷
格式化输出缺陷
数据劫持
检测
5 漏洞防御
混淆加壳
访问控制
DEP
GS
ASLR
safeSEH
CFG
CIG
ACG

图 1 课程的教学内容