

# CCERT介绍与 近期安全热点问题

中国教育和科研网紧急响应组 (CCERT)

清华大学信息网络工程研究中心

郑先伟

电子邮件: [zxw@cernet.edu.cn](mailto:zxw@cernet.edu.cn)

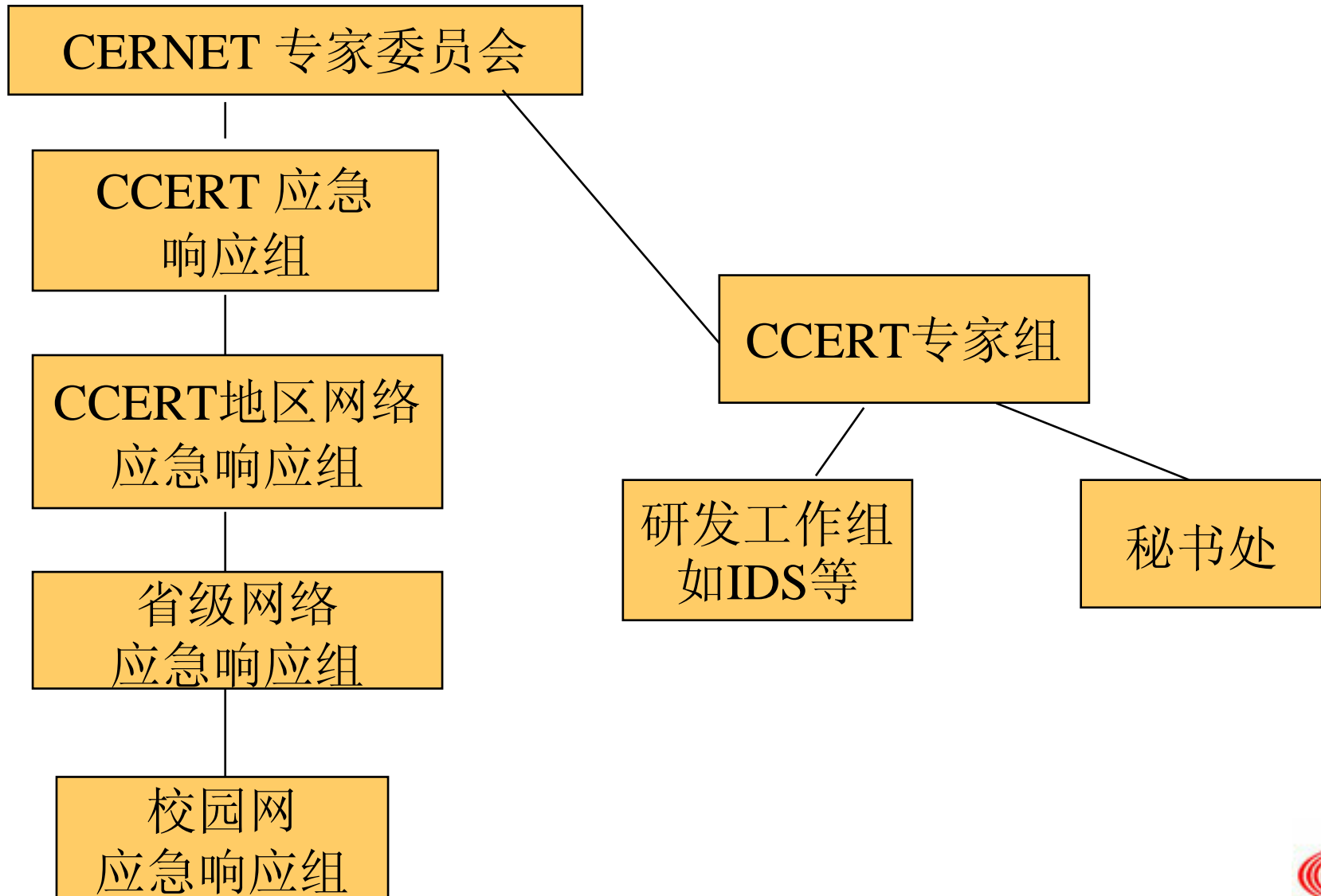
电 话: 010-62784301

传 真: 010-62785933

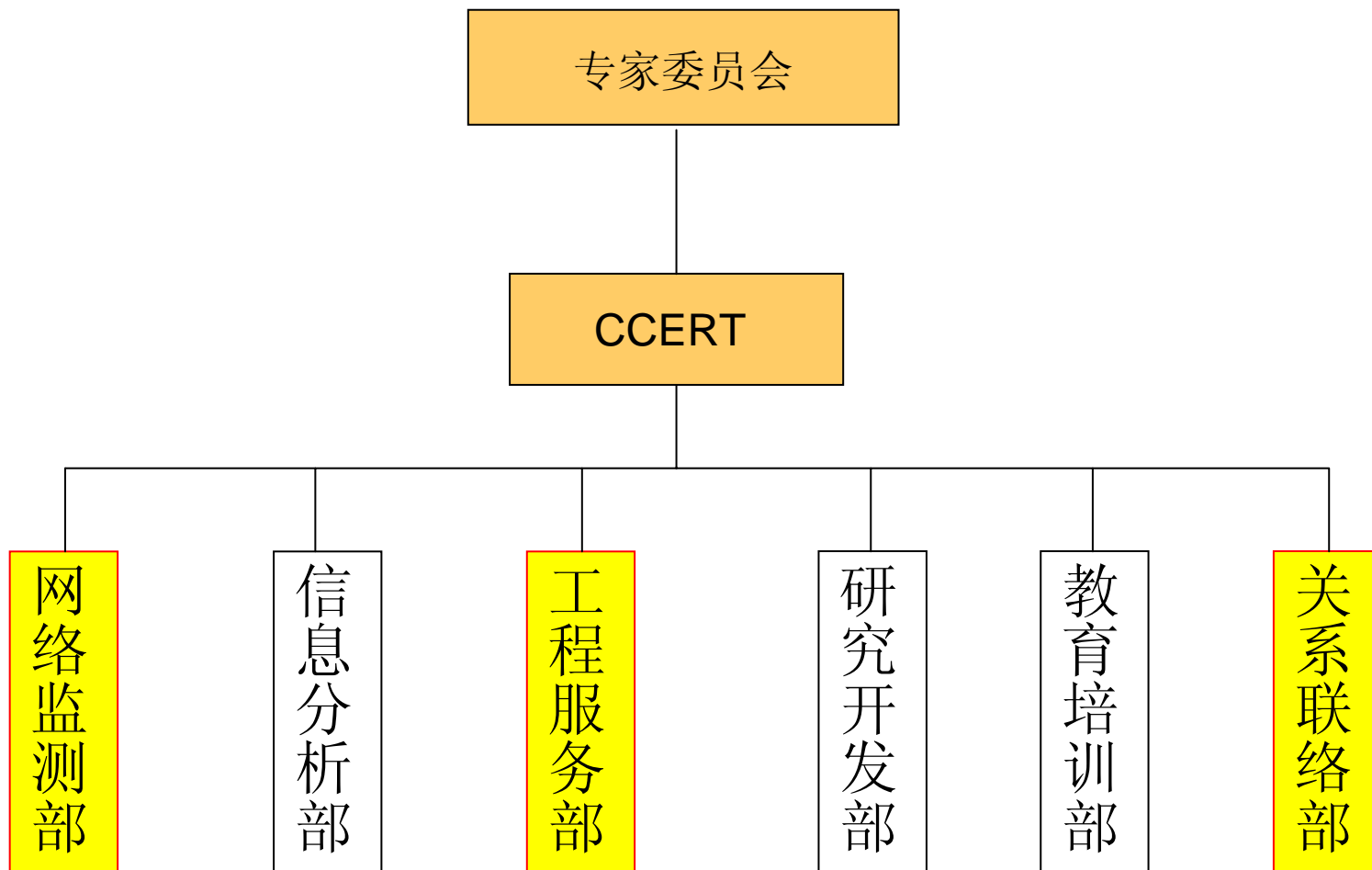
地 址: 清华大学FIT大楼1区213

- 
- A red arrow points to the first item in the list.
1. CCERT的组织建设及功能
  2. 近期安全热点问题

# CCERT组织结构建设



# CCERT 组织结构



Network monitoring, engineering, analysis, R&D, Awareness/training, Liaison

- CERNET主干网、清华大学校园网安全监控
- 安全信息的收集、整理和分析. 跟踪网络安全动态, 发布安全公告
- 安全事件的处理和协调
- 安全技术咨询
- 安全技术的培训和技术交流
- 网络安全技术相关的研究和开发

- CERNET省级节点网安全监控
- 跟踪网络安全动态，及时预警
- 安全事件的处理和协调
- 安全技术咨询
- 安全技术的培训和技术交流
- 网络安全技术相关的研究和开发（协同合作方式）

- 信息库、信息发布平台（CERT网站）

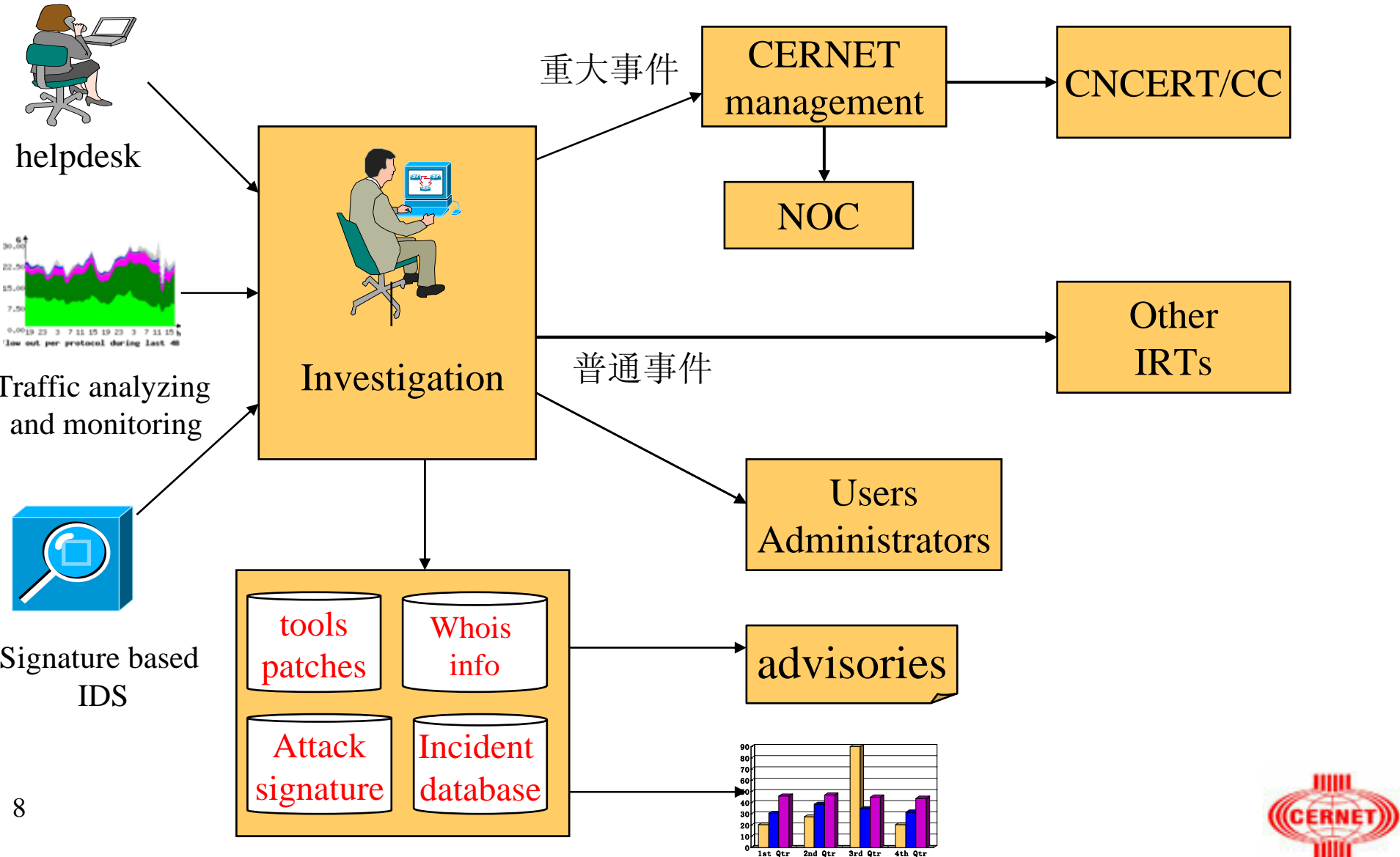
<http://www.ccert.edu.cn>

- 电话、电子邮件

6278401 incidentreport@ccert.edu.cn

- 事件处理系统
- 流量监控系统
- 入侵检测系统

# 应急响应流程



- ① 应急信息建设维护——准备
- ② 事件的报告与检测——检测
- ③ 事件的调查与分析——分析
- ④ 管理层决策与协调——决策
- ⑤ 网络的控制与隔离——控制
- ⑥ 信息的通报与联系——通告
- ⑦ 事后的统计与分析——统计

1. CCERT的组织建设及功能

→ 2. 近期安全热点问题

# 当前安全形势

- 表面现象——很长时间都没有大规模的蠕虫爆发,互联网看似风平浪静,一片歌舞升平,难道是所有的病毒作者都改邪归正了?
- 实际情况——病毒木马仍然大量存在,危害比以前更大,编写病毒人并没改邪归正,相反在利益的驱使下越来越多的人参与到这个行列当中来

- 可以获取经济利益的“商业病毒木马”泛滥

病毒编写者不再单纯炫耀技术，而更多以经济利益为目的。跟过去那种恶性病毒突然爆发相比，目前这种“悄悄潜入”的“商业病毒”给全社会造成了更大的实际损失。

- 病毒传播范围小，目的性和针对性更强

现阶段的病毒不同以往，它们不会毫无目的的爆发，相反只影响很小的一部分区域。对于黑客来讲控制小范围的计算机所带来的利益已经足够，并且风险要小得多。这样也给反病毒软件查杀带来一定的困难

- 传播方式更加先进，利用社会工程学原理等新手法传播

通过即时通讯工具、网页、电子邮件传播成为新的传播手段，原有的通过网络扫描传播的方式因为影响太大已经越来越不被采用

- 隐藏和生存能力加强

Rootkits技术被病毒编写者所广泛应用。它们通过修改系统内核或取得系统最高权限，从而将自身、内存数据和注册表信息隐藏起来，躲避杀毒软件对其进行检测。

一旦感染，自动关闭系统杀毒软件

- 编写简单化和生产产业化

网络到处可以下载到木马源程序，你只要稍微改一改就可以实现自己想要的功能，如果你对编程一窍不通，也没有关系，只要给钱我们完全可以按照你提的要求为你订制木马程序

- 新的攻击方式呈出不穷

网络钓鱼(phishing)

僵尸网络(botnet)

基于80端口的攻击-SQL注入(SQL Injection)  
等

- 僵尸网络(botnet)

僵尸网络（Botnet），是指采用一种或多种传播手段，将大量主机感染bot程序（僵尸程序），从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。

- 网络钓鱼 (Phishing)

“网络钓鱼”攻击利用欺骗性的电子邮件和伪造的Web站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如信用卡号、账户用户名、口令和社保编号等内容。诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等可信的品牌，在所有接触诈骗信息的用户中，有高达5%的人都会对这些骗局做出响应。

- 什么是 SQL注入(SQL Injection)

假设某个 Web 站点上有了一个允许访问者对联机数据库搜索特定词语的应用程序。并且该应用程序是这样工作的：接受用户提供的任何输入内容，将此内容插入一个数据库查询，然后就运行该查询；不过，攻击者可能会提供 SQL 语句，而不是文本。这样，当 Web 应用程序运行查询时，攻击者的命令就会作为查询的一部分执行。这种类型的漏洞即所谓 SQL 注入。

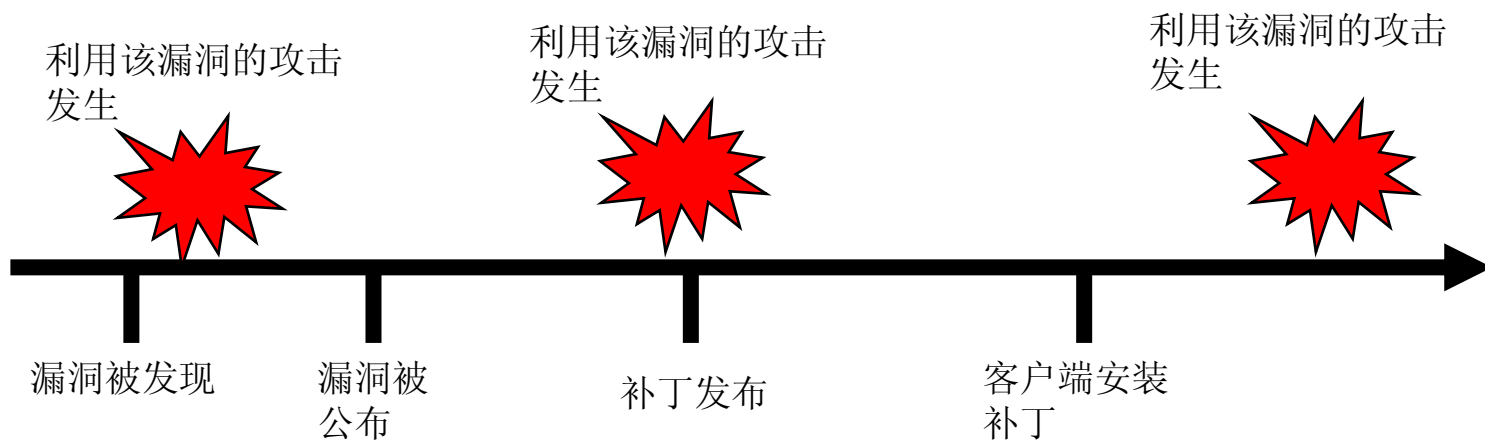
- `strSQL="SELECT * FROM tblUser WHERE  
UserName=' " & _  
Request("UserName") & "' AND Password=' " &_  
Request("Pass") & "' "`
- ' 直接交给SQL Server执行，这是最危险的地方
- `Set rec=cnn.Execute(strSQL)`
- `If NOT rec.EOF Then`

- 网页希望通过页面获得用户提交的用户名和密码，并与数据库中的结果比较以判断用户是否合法，如果我在用户名的输入框内输入如下admin;
- 结果就是**SELECT \* FROM tblUser**
- **WHERE UserName='admin; ' AND Password='asdf'**

- 越来越多的IE,office等软件的漏洞被公布出来

利用这类漏洞可以有效地穿透防火墙

- 零时间攻击和未知攻击增多



- 一切都是为了经济利益
- 手段越来越高明
- 方式越来越多
- 危害程度越来越大
- 检测和控制难度越来越高

- ARP木马程序

一个用来盗窃传奇游戏帐号的木马

导致局域网频繁掉线

- ARP的原理

ARP是地址转换协议（Address Resolution Protocol）的英文缩写，它是一个链路层协议，工作在OSI模型的第二层，在本层和硬件接口间进行联系，同时对上层（网络层）提供服务。

- 工作机理

主机名	IP地址	MAC地址
主机A	192.168.1.2	01-01-01-01-01-01
主机B	192.168.1.3	02-02-02-02-02-02
网关C	192.168.1.1	03-03-03-03-03-03
主机D	10.1.1.2	04-04-04-04-04-04
网关E	10.1.1.1	05-05-05-05-05-05

# 校园网近期热点安全问题

- 假如主机A要与主机B通讯，它首先会检查自己的ARP缓存中是否有192.168.1.3这个地址对应的MAC地址，如果没有它就会向局域网的广播地址发送ARP请求包，大致的意思是192.168.1.3的MAC地址是什么请告诉192.168.1.2,而广播地址会把这个请求包广播给局域网内的所有主机，但是只有192.168.1.3这台主机才会响应这个请求包，它会回应192.168.1.2一个arp包，大致的意思是192.168.1.3的MAC地址是02-02-02-02-02-02。这样的话主机A就得到了主机B的MAC地址，并且它会把这个对应的关系存在自己的ARP缓存表中。之后主机A与主机B之间的通讯就依靠两者缓存表里的MAC地址来通讯了，直到通讯停止后两分钟，这个对应关系才会被从表中删除。

# 校园网近期热点安全问题

再来看一个非局域网内部的通讯过程，假如主机A需要和主机D进行通讯，它首先会发现这个主机D的IP地址并不是自己同一个网段内的，因此需要通过网关来转发，这样的话它会检查自己的ARP缓存表里是否有网关192.168.1.1对应的MAC地址，如果没有就通过ARP请求获得，如果有就直接与网关通讯，然后再由网关C通过路由将数据包送到网关E，网关E收到这个数据包后发现是送给主机D（10.1.1.2）的，它就会检查自己的ARP缓存（没错，网关一样有自己的ARP缓存），看看里面是否有10.1.1.2对应的MAC地址，如果没有就使用ARP协议获得，如果有就是用该MAC地址与主机D通讯。

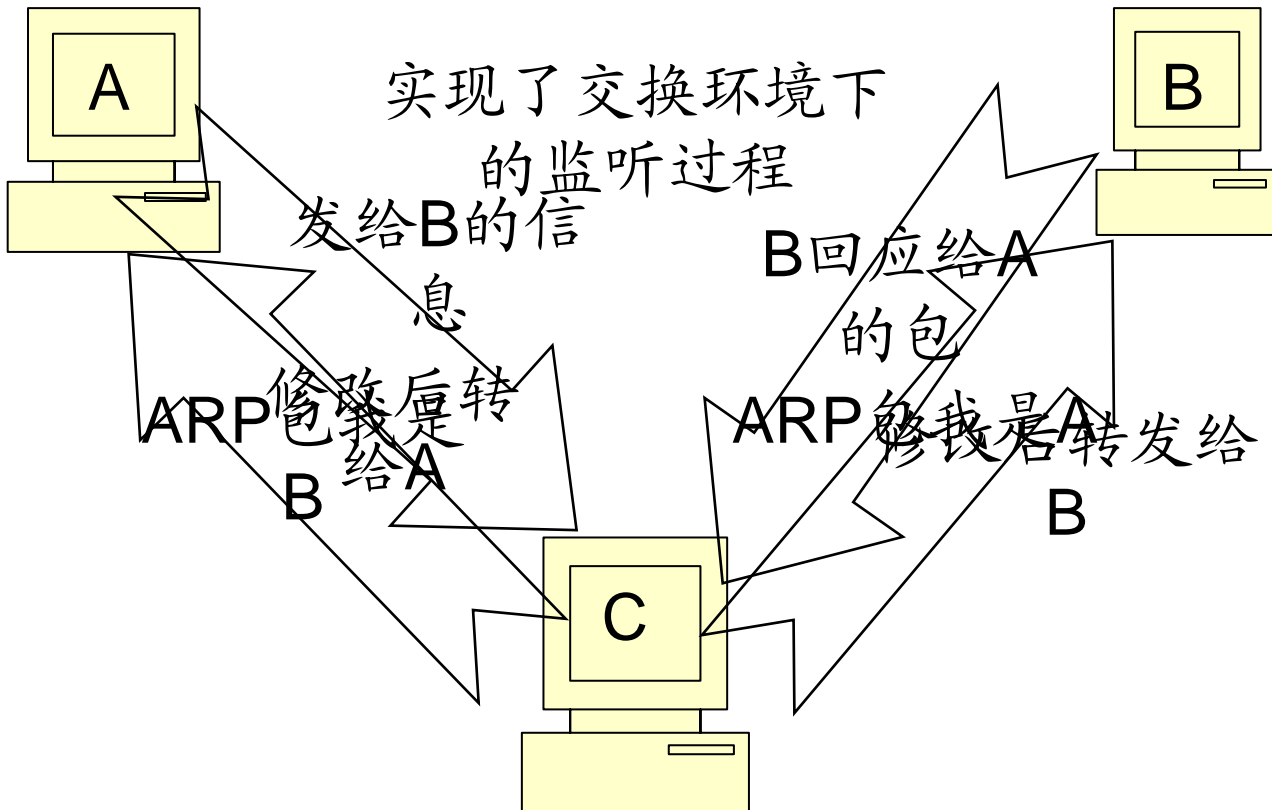
- Arp欺骗原理

主机在实现ARP缓存表的机制中存在一个不完善的地方，当主机收到一个ARP的应答包后，它并不会去验证自己是否发送过这个ARP请求，而是直接将应答包里的MAC地址与IP对应的关系替换掉原有的ARP缓存表里的相应信息。这就导致主机B截取主机A与主机D之间的数据通信成为可能。

# 校园网近期热点安全问题

- 首先主机B向主机A发送一个ARP应答包说192.168.1.1的MAC地址是02-02-02-02-02-02，主机A收到这个包后并没有去验证包的真实性而是直接将自己ARP列表中的192.168.1.1的MAC地址替换成02-02-02-02-02-02，同时主机B向网关C发送一个ARP响应包说192.168.1.2的MAC是02-02-02-02-02-02，同样网关C也没有去验证这个包的真实性就把自己ARP表中的192.168.1.2的MAC地址替换成02-02-02-02-02-02。当主机A想要与主机D通讯时，它直接把应该发送给网关192.168.1.1的数据包发送到02-02-02-02-02-02这个MAC地址，也就是发给了主机B，主机B在收到这个包后经过修改再转发给真正的网关C，当从主机D返回的数据包到达网关C后，网关也使用自己ARP表中的MAC，将发往192.168.1.2这个IP地址的数据发往02-02-02-02-02-02这个MAC地址也就是主机B，主机B在收到这个包后再转发给主机A完成一次完整的数据通讯，这样就成功的实现了一次ARP欺骗攻击。

- ARP欺骗



- 局域网内一旦有ARP的攻击存在，会欺骗局域网内所有主机和网关，让所有上网的流量必须经过ARP攻击者控制的主机。其他用户原来直接通过网关上网现在转由通过被控主机转发上网，由于被控主机性能和程序性能的影响，这种转发并不会非常流畅，因此就会导致用户上网的速度变慢甚至是频繁的断线。另外ARP欺骗需要不停的发送ARP应答包，会造成网络拥塞。

## 目前的解决办法:

到有问题的局域网内去抓包, 然后找出感染的机器.

在交换机的所有端口上绑定唯一MAC

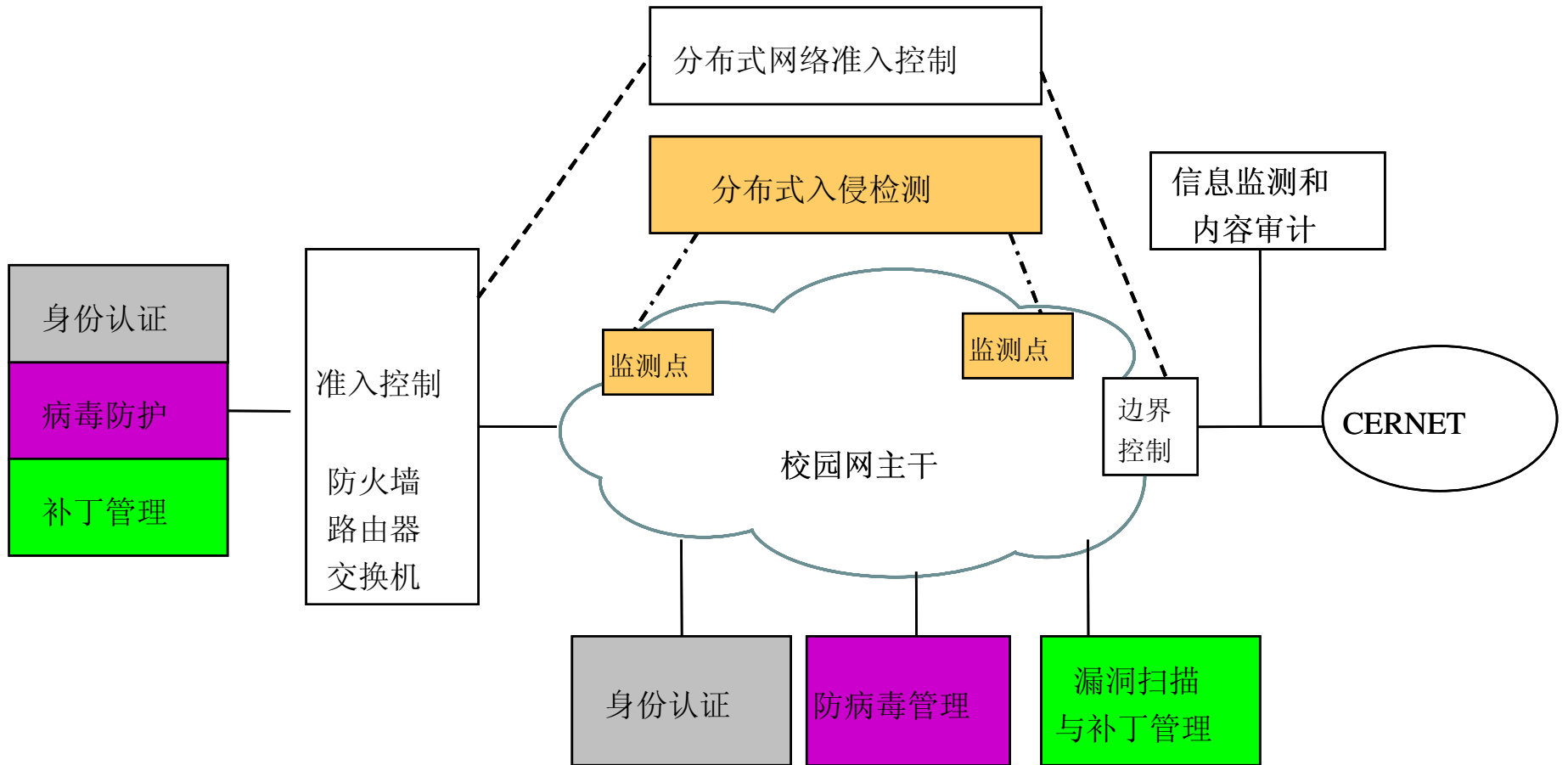
- 但是上述方法是被动的,一般都是出了问题才去采取措施,我们需要为校园网建立一个有效的检测与控制机制,将问题防范于未然.
- 这就提出了一个目前比较流行的概念:

准入控制机制

# 校园网近期热点安全问题

- 一个基本的准入控制系统应该包含以下部分
  1. 用户入网身份认证系统;
  2. 计算机补丁管理和安全漏洞扫描系统;
  3. 分布式入侵检测系统;
  4. 分布式的网络准入控制系统;
  5. 集中管理的病毒防护系统;
  6. 网络不良信息监测和内容审计系统

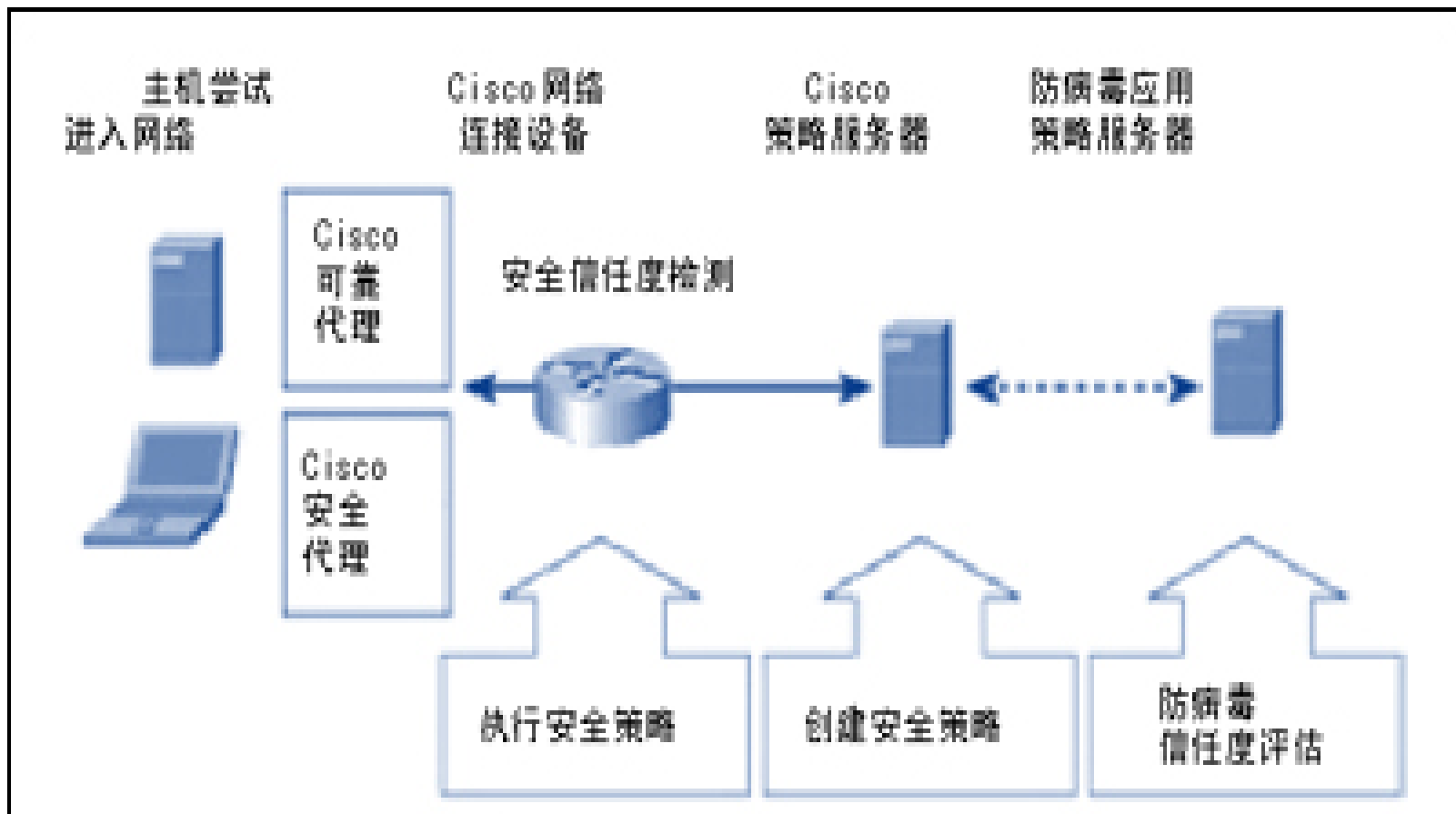
# 校园网近期热点安全问题



一个基本的准入控制框架

- 目前比较成熟的准入控制体系都是基于802.1X协议实现的.
- 如CISCO的NAC (Network Admission Control)
- 华为的EAD (Endpoint Admission Defense )

- CISCO的NAC系统结构



## • 华为的EAD

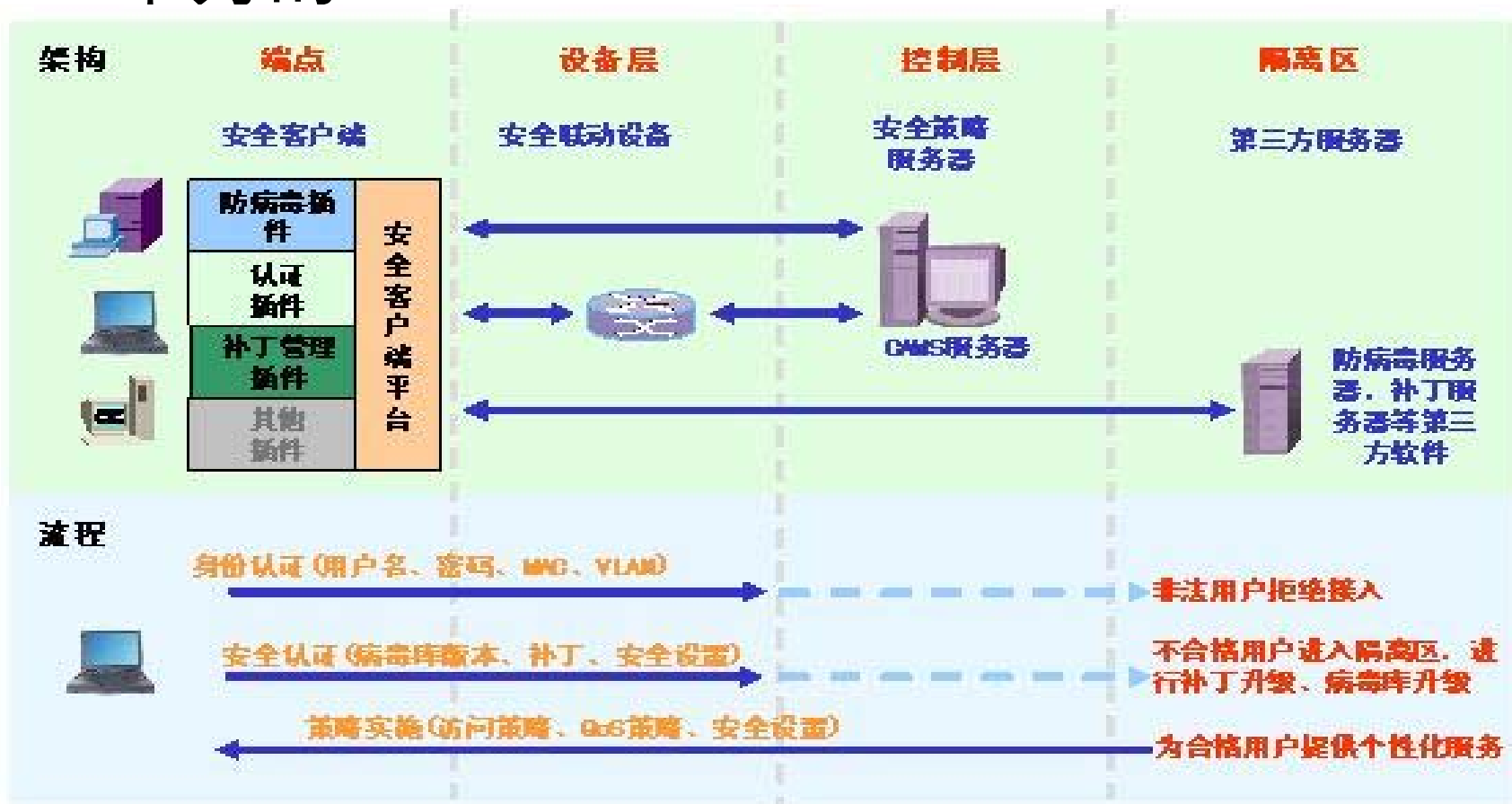


图1 EAD 基本原理

- 除了802.1X协议外,还有其他一些形势的准入控制,如微软在他的下一代操作系统vista中就内置了准入控制体系.

# 总结

- 网络安全状况不容乐观
- 我们需要建设一个更加完善的校园网安全体系去应对未来的网络

谢谢

