CERNET第二十三届学术年会

校园网安全应急响应能力测试

清华大学 网络科学与网络空间研究院
中国教育和科研计算机网应急响应组
张　甲
2016年10月24日

报告提纲

- 研究背景
- 测试方案设计
- 测试结果分析
- 相关问题讨论
- 结论

研究背景——问题的提出

- 一次安全事件处理
  - 在研究过程中发现某院系网站页面被篡改
  - 通知院系管理员处置
  - 从发现到修复历时一个多月

研究背景——问题的提出

- 一次常规的校园网治理工作
  - 发现校园网部分DNS服务器配置不当，有进行反射攻击的可能性
  - 信息化主管部门、各院系网络管理员、校园网运维部门共同参与
  - 历时两个月基本完成治理
- 问题
  - 校园网出现安全事件应该通过什么渠道通报？
  - 如果有多个渠道，哪个渠道更有效？
  - 面对不同的安全事件，各类渠道的应对策略和态度是否一致？
  - 现有渠道还存在哪些问题？

研究背景

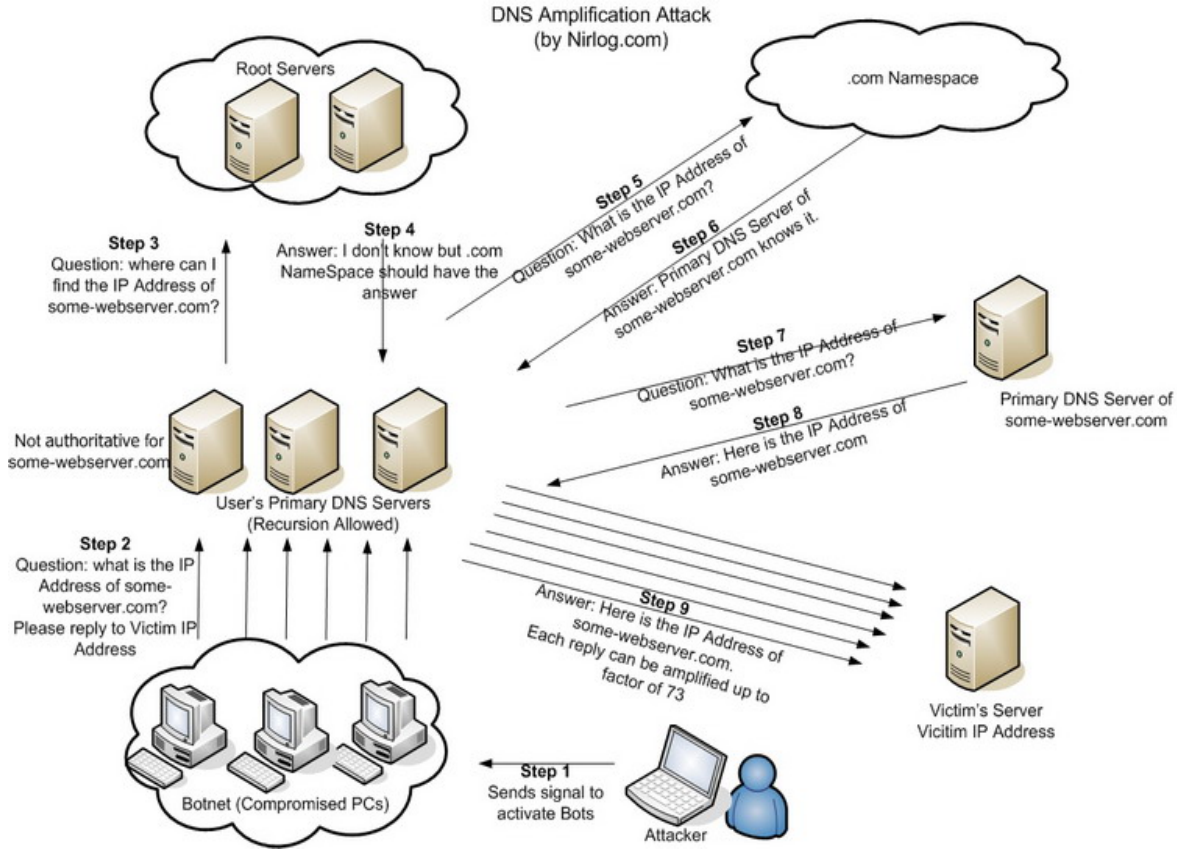
- You’ve Got Vulnerability: Exploring Effective Vulnerability Notifications, *USENIX Security 2016*
- 我们计划做一个类似的测试
  - 测试目标：CERNET内部各高校校园网
  - 测试方法：利用不同的通报渠道通报不同的安全事件，观察最终的事件响应效果
  - 测试目的：研究影响安全应急响应能力的因素，提出相应的改进建议

测试方案设计——漏洞选择

- 漏洞类型要具有代表性
  - 基础设施漏洞、Web应用漏洞、应用系统漏洞
- 威胁程度要有层次感
  - 高危事件、中危事件、低危事件
- DNS Any Query Response
  - 基础设施漏洞、低危漏洞
- 打印机远程控制
  - 应用系统漏洞、中危漏洞
- Web网页篡改
  - Web应用漏洞、高危漏洞

测试方案设计——漏洞选择

- DNS Any Query Response
  - 一种利用DNS配置不当进行DDOS反射攻击的方法



测试方案设计——漏洞选择

- 打印机远程控制
  - 由于配置不当导致攻击者可以远程控制打印机

测试方案设计——漏洞选择

- Web网页篡改
  - 利用Web应用漏洞将博彩、色情、枪支、毒品等非法内容嵌入高校网站
  - 搜索引擎：site:edu.cn 六合彩

测试方案设计——渠道选择

- 赛尔网络

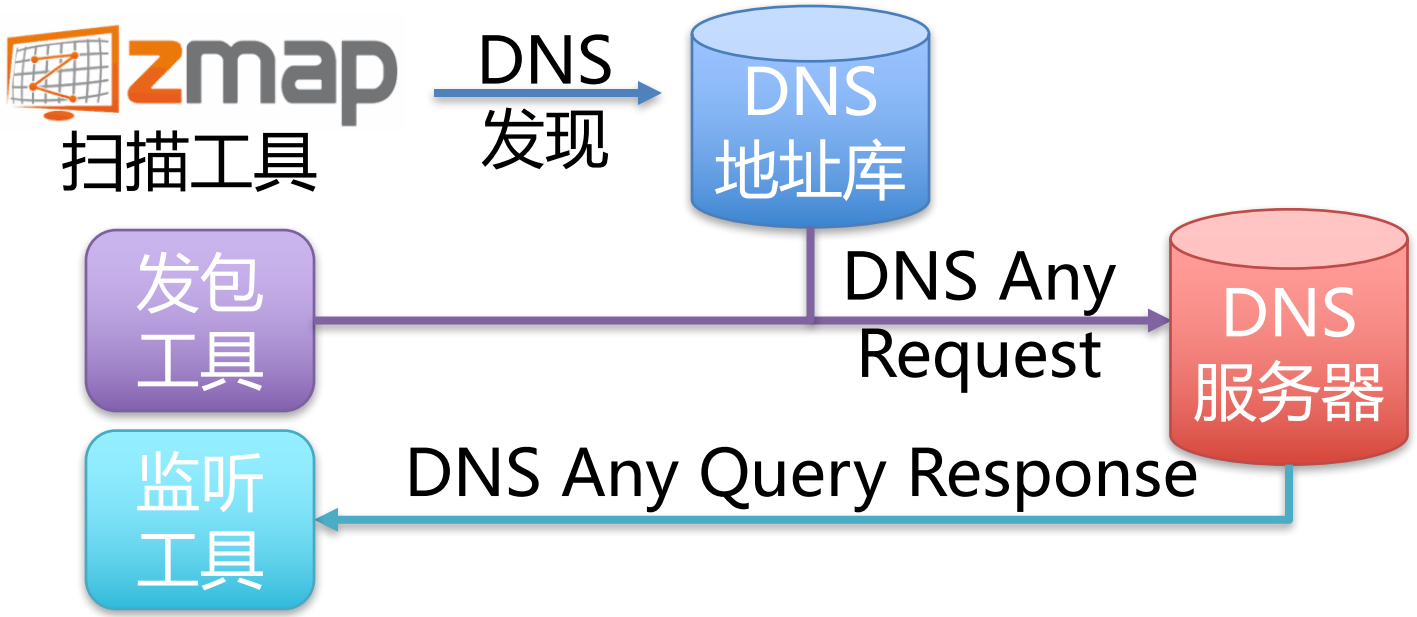
  - 拥有最为全面的通信方式，可以确保任一IP地址、任一单位的安全事件都可以找到联系人（电话or邮件）
- 安全应急响应邮件列表

  - 中国高校网络信息安全工作组基础数据库
  - http://ipdb.sec.edu-info.edu.cn/ipdb
- 校园网运维即时通信群

  - QQ交流群：49922019

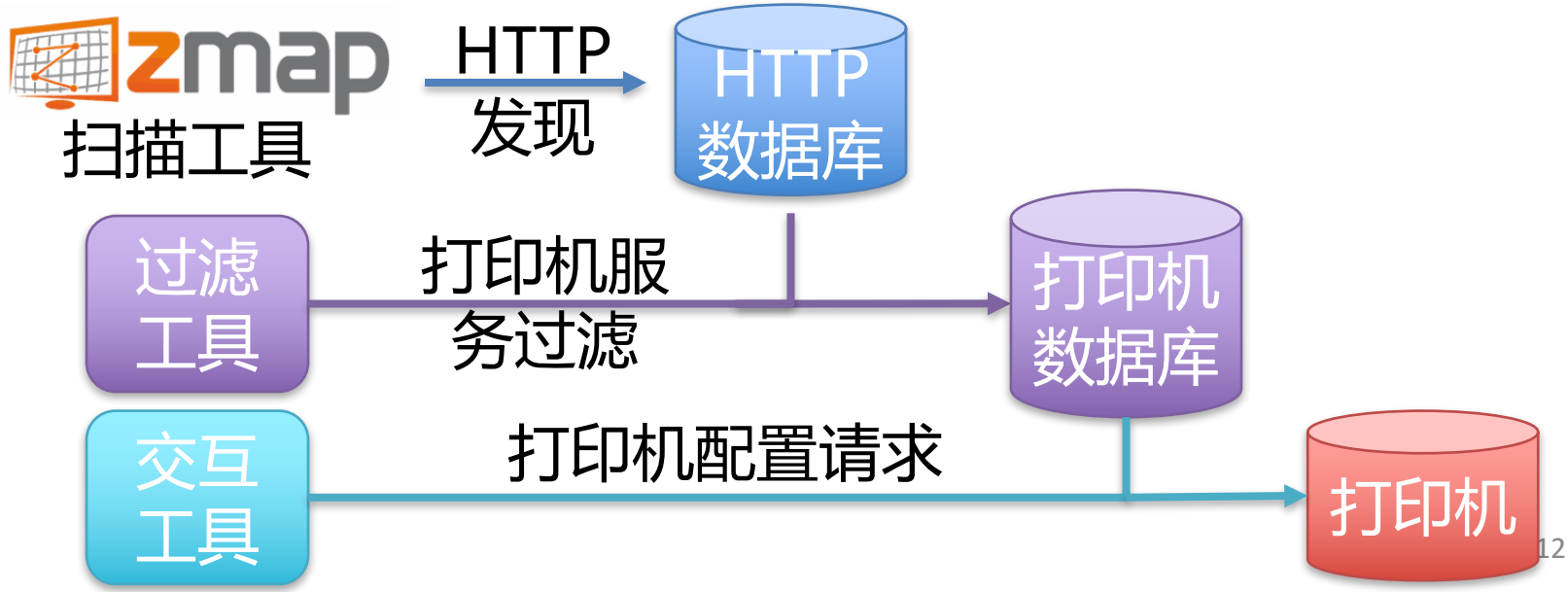
测试方案设计——漏洞采集

- DNS Any Request 扫描
  - 利用扫描工具获取教育科研网范围内的DNS服务器地址
  - 向DNS服务器发送DNS ANY Request请求，并监听反馈信息
  - 如果返回超长包，则认为该DNS存在反射攻击风险



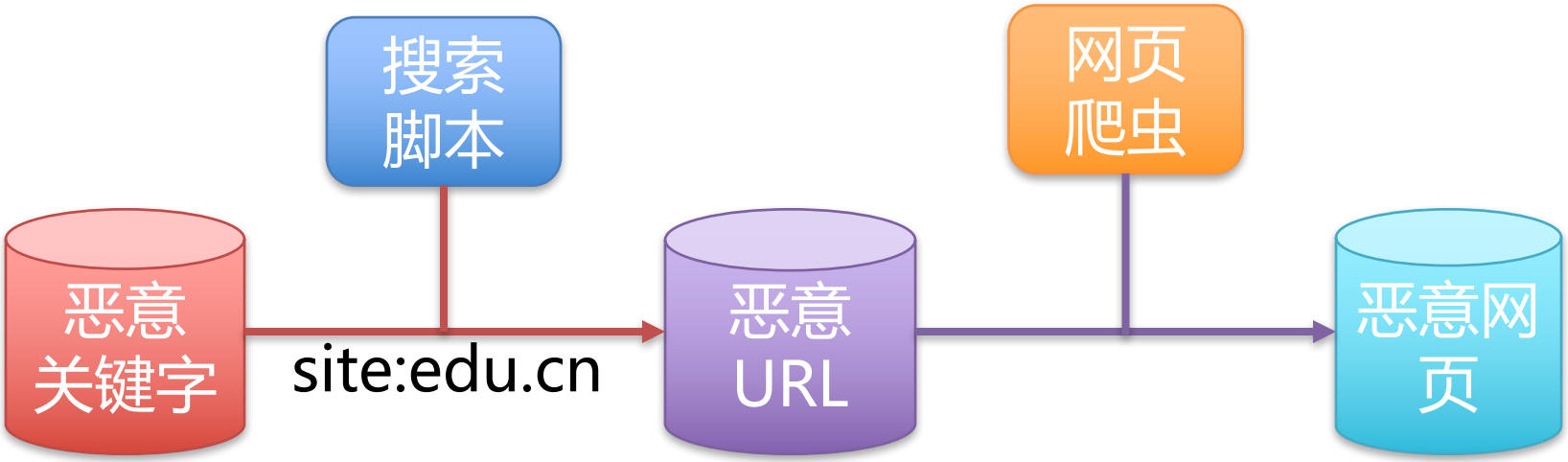
测试方案设计——漏洞采集

- 打印机远程扫描
  - 利用扫描工具获取教育科研网范围内80端口开放的服务器基本信息
  - 过滤其中包含打印机主页信息的地址
  - 利用脚本向打印机控制页面发送配置请求，能够成功打开配置页则认为存在任意配置风险

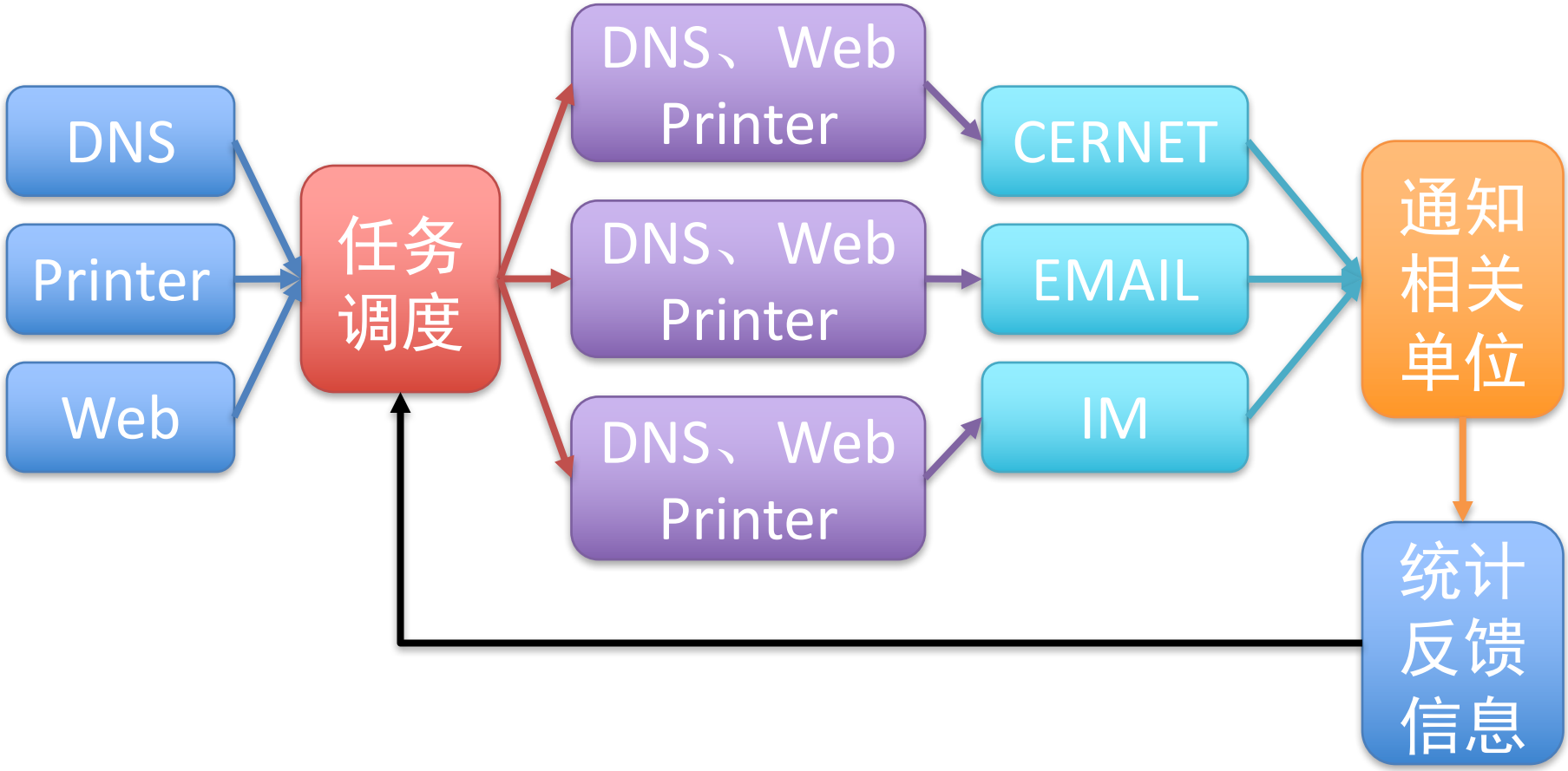


测试方案设计——漏洞采集

- 恶意网页爬取
  - 通过第三方公司获得大量恶意搜索关键字
  - 利用搜索引擎定向搜索功能，在edu.cn域名下搜索各类恶意关键字
  - 将搜索到的网页利用爬虫爬取，能够成功获取网页的则认为该网站已被恶意篡改



测试方案设计——测试流程


DNS
Printer
Web
任务调度
DNS、Web Printer
DNS、Web Printer
DNS、Web Printer
CERNET
EMAIL
IM
通知相关单位
统计反馈信息

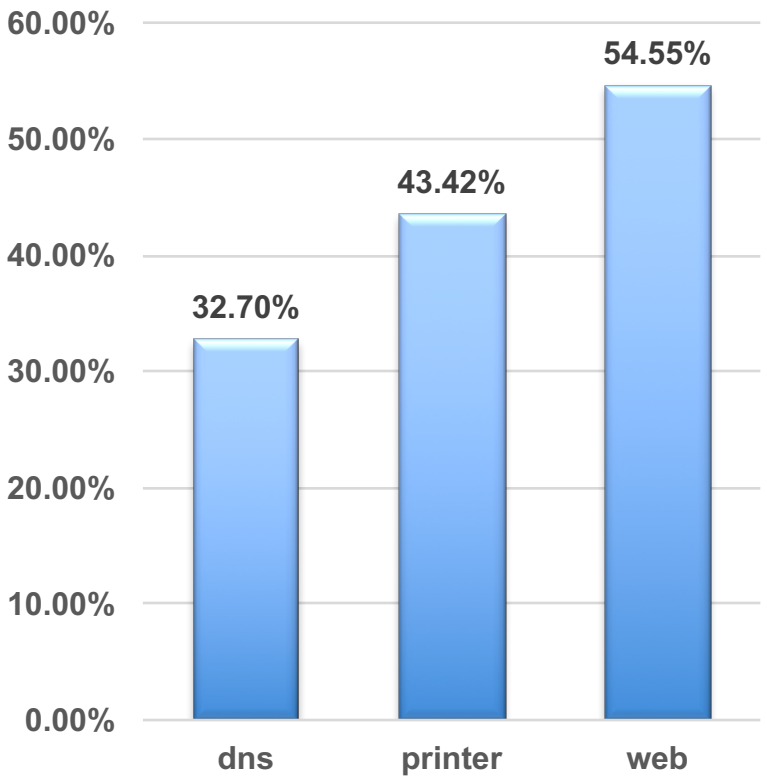
测试结果分析

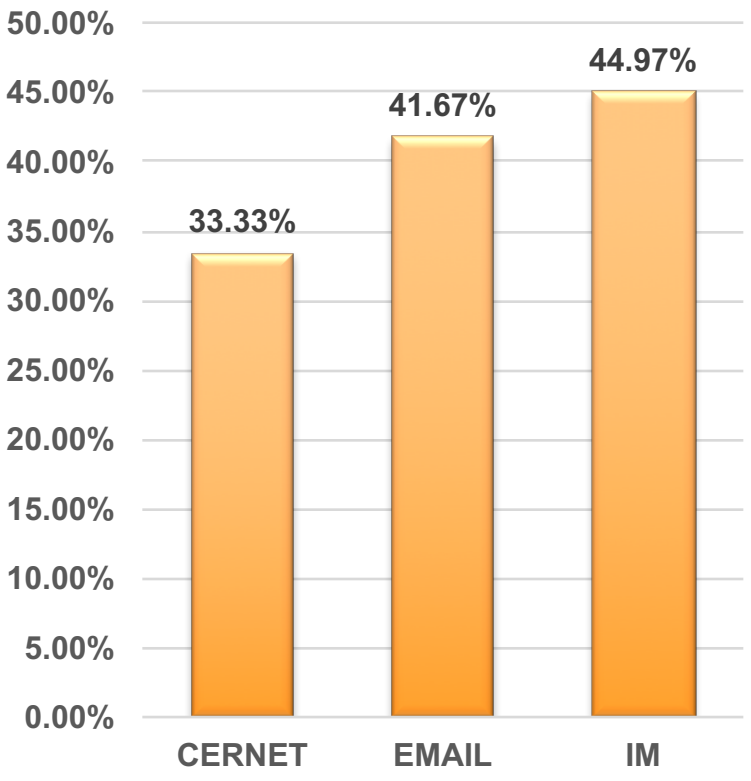
- 发现各类漏洞共2292个
  - DNS ANY Query Response 961个，涉及531个单位
  - 打印机远程控制漏洞 178个，涉及60个单位
  - Web恶意网页篡改1153个，涉及86个单位

	DNS ANY Query	打印机远程控制	Web恶意网页
漏洞数量	961	178	1153
机构数量	531 高校：452 政府：18 其他：61	60 高校：47 政府：6 其他：7	87 高校：79 政府：1 其他：6

测试结果分析

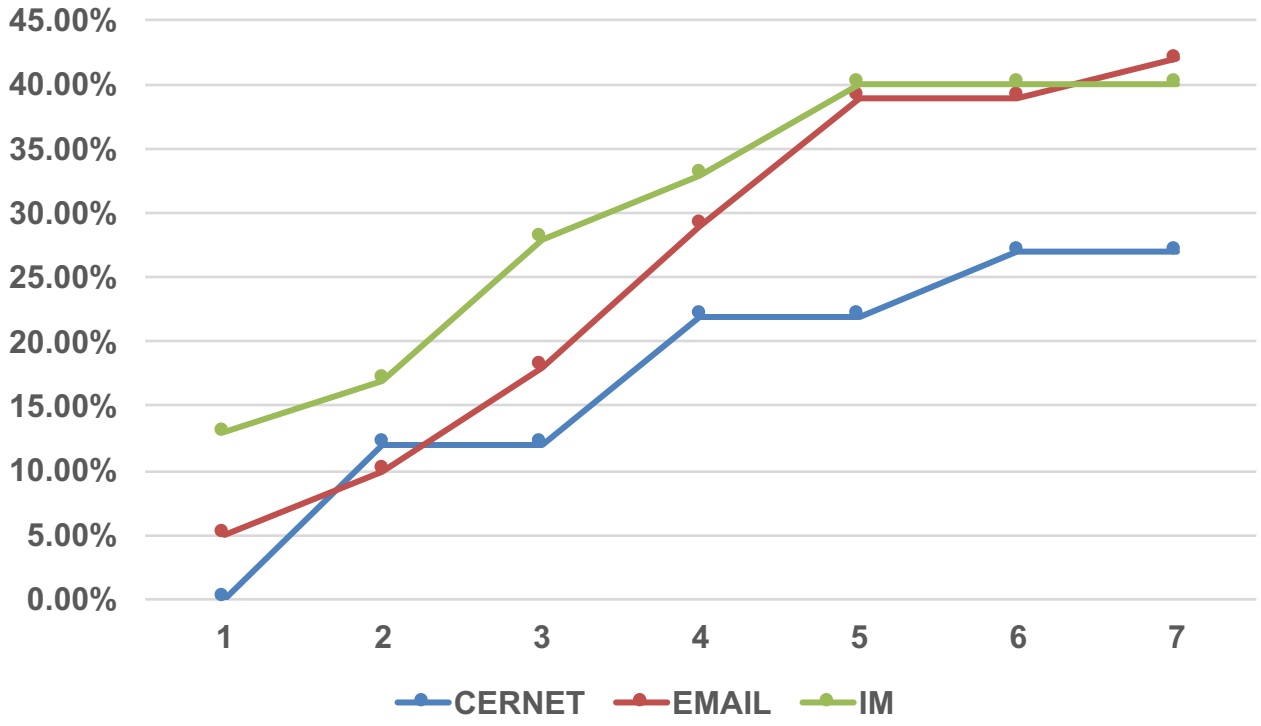
- 首轮应急响应处置结果（按机构统计，一周）





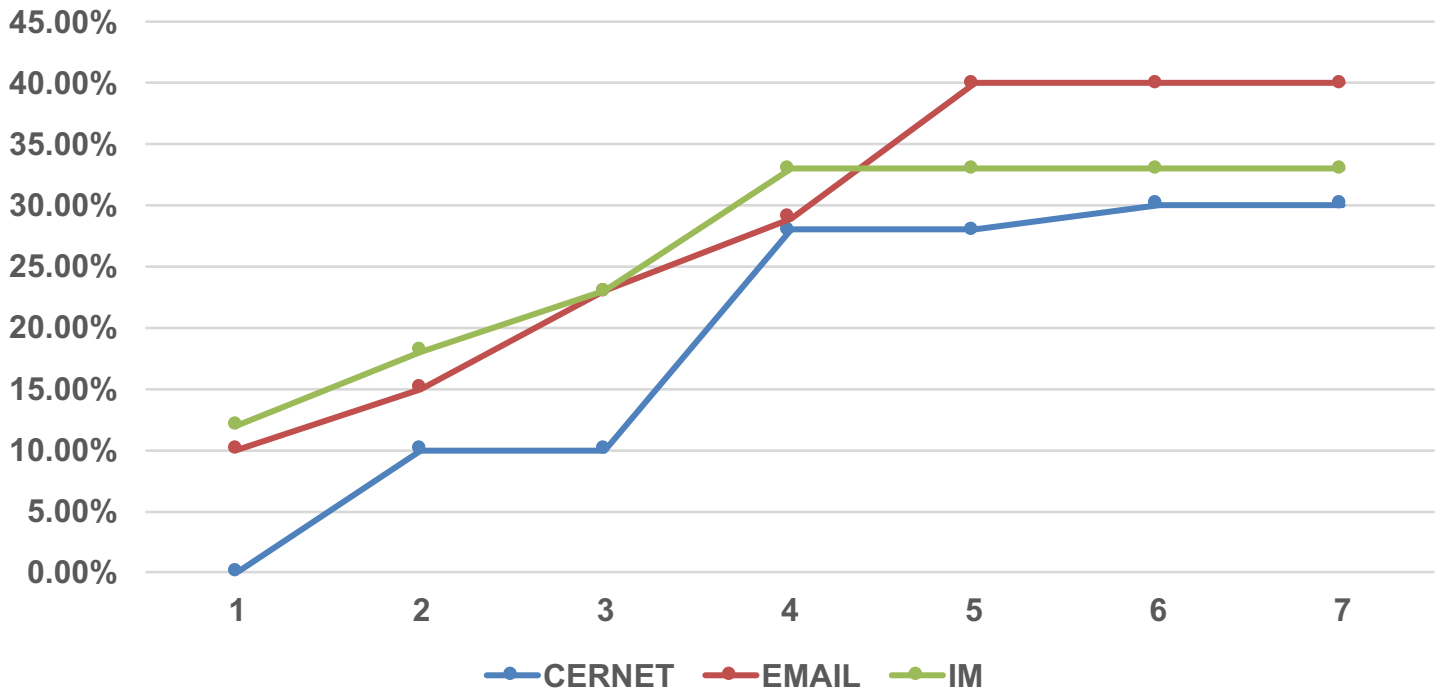
测试结果分析

- 时效性（DNS ANY QUERY Response）
  - 即时通信方式响应速度最快
  - 邮件通知最终的修复比率最高



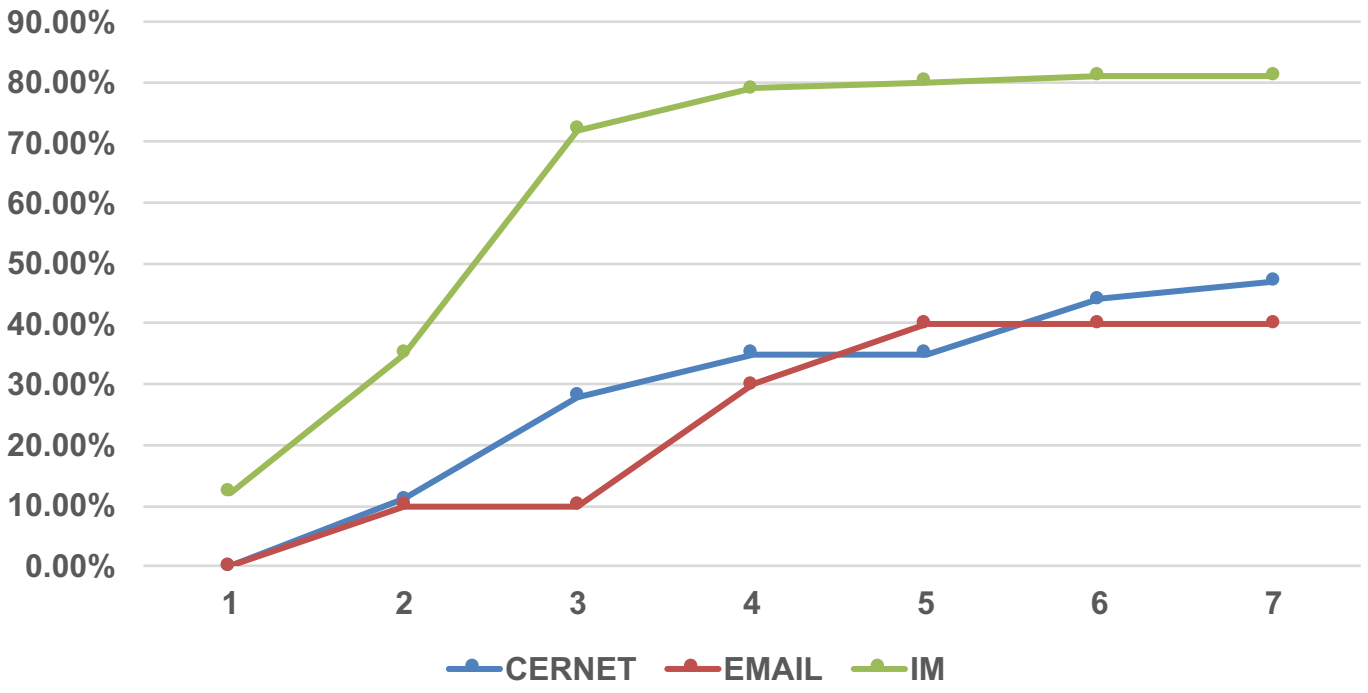
测试结果分析

- 时效性（打印机远程控制）
  - 即时通信响应速度最快
  - 邮件具有持续的响应，最终修复比最高



测试结果分析

- 时效性（恶意网页篡改）
  - 即时通信响应速度最快，修复时间集中且比例高
  - 客服通知具有持续的响应

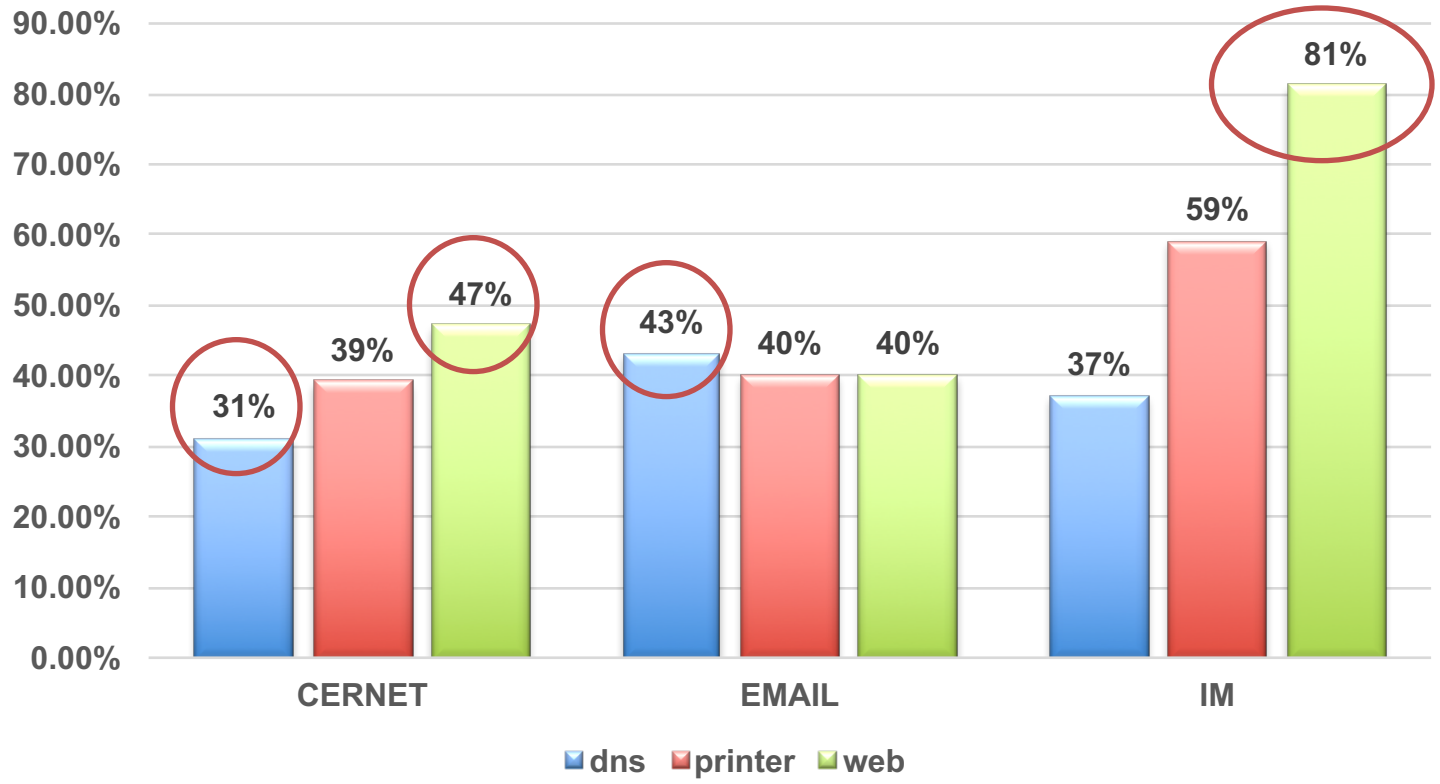


测试结果分析

- 初步结论
  - 即时通信手段效果相对最好
  - 客服通知以及Email通知对不同的漏洞表现出了不同的结果
- 问题
  - 不同的漏洞在同一个渠道通知下，修复速度、比例具有很大的不同，为什么？
  - 同一个漏洞，在不同渠道下响应速度，修复比例差异很大，为什么？

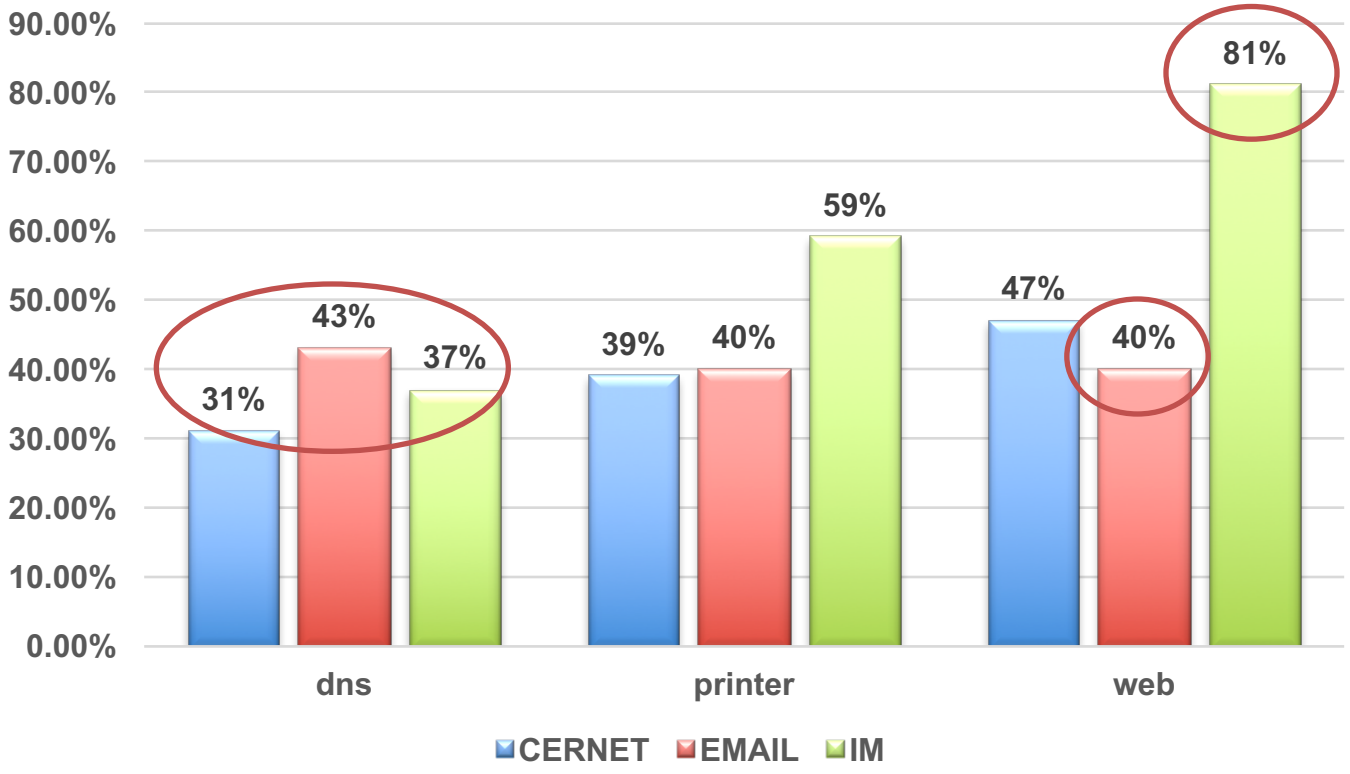
相关问题讨论——渠道差异性

- 技术渠道有利于技术问题，管理渠道有利于业务问题
- 即时通信效果优于非即时通报手段
- 群组更有利于解决问题



相关问题讨论——漏洞差异性

- 高危漏洞总体响应效果要好，但同时受限于渠道的权限
- 中低危漏洞响应主要受限于响应团队技术能力

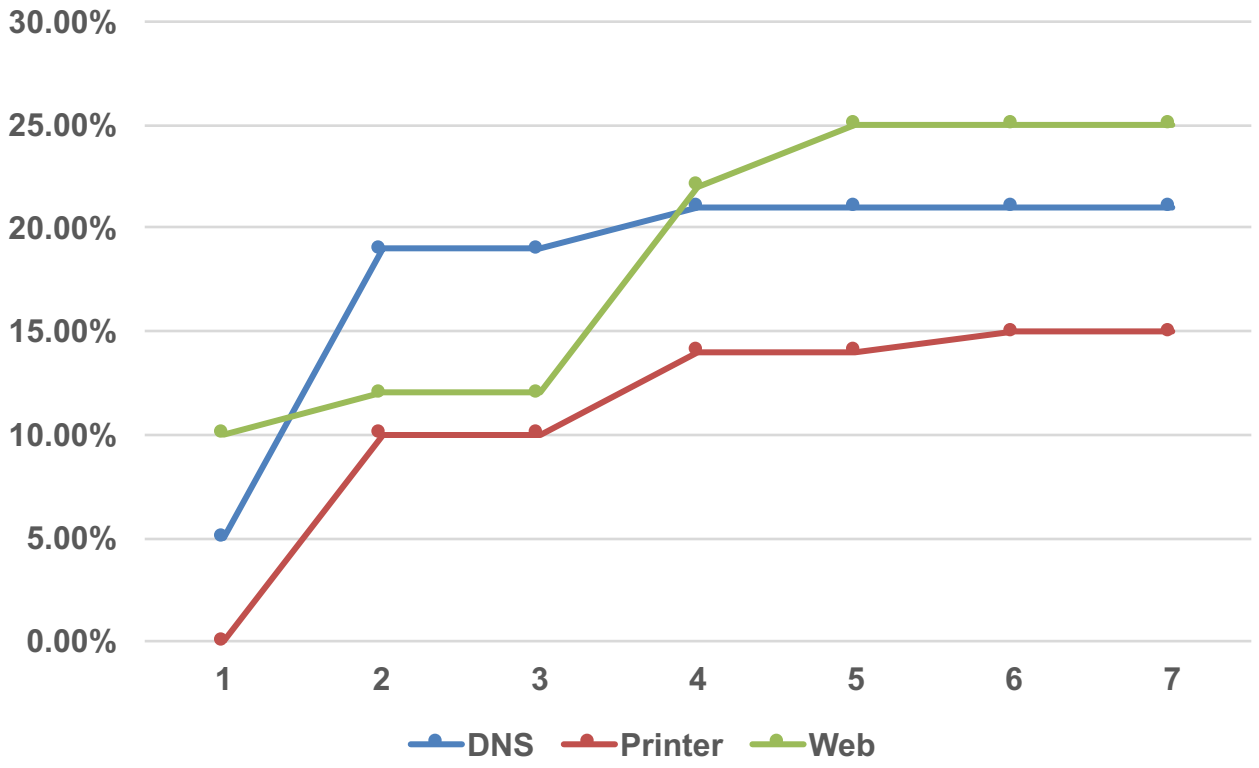


相关问题讨论——机构差异性

- 本次测试主要对象是高校，但是部分政府机构以及研究机构和企业也在测试范围之内
  - 政府机构的响应速度以及修复比例最高
  - 其他机构的修复比例相比高校稍高
  - 重点院校相比一般院校的修复比例要高，但是出现问题较多的重点高校完全修复的程度较低

相关问题讨论——通知次数的影响

- 多通知一轮会有部分改进，但是影响有限



相关问题讨论——改进建议

- 建立更加有效的即时应急响应渠道
  - 加强即时通信工具在应急响应工作中的作用，扩大覆盖面
- 建立群组化的应急响应团队
  - 建立虚拟化的应急响应团队，多部门、多层级的相关人员都应当参与到应急响应工作中来
  - security@xxx.edu.cn
- 加强技术培训
  - 提高应急响应团队的技术能力，对常见安全问题能够在第一时间进行应急处理

结 论

- 主要工作
  - 利用3种不同等级的漏洞测试了校园网3类主要应急响应渠道的响应能力
- 主要结论
  - 即时通信方式对应急响应的作用最为明显
  - 应急响应水平需要考虑通知渠道所对应的业务权限、技术水平等
  - 找到正确的处理渠道胜于多次无效的通告
- 建议
  - 建立覆盖范围更广的应急响应即时通信渠道
  - 扩大应急响应参与人员的范围
  - 加强一线应急响应人员的技术培训

广告时间

- 邮件列表
  - 中国高校网络信息安全工作组基础数据库
  - http://ipdb.sec.edu-info.edu.cn/ipdb
  - 姚星昆：yaoxk@tsinghua.edu.cn
- QQ交流群：49922019
  - 高校校园网交流
  - 学校 + 姓名 验证

广告时间

EDU IPDB 首页 增加 排行榜 地区管理 全国搜索 退出 关于

排行榜

排名	地区	注册单位数量	注册联系人数量	未注册单位数量	完成百分比	单位总数
1	吉林省	37	47	37	0.50	74
2	北京市	56	88	65	0.46	121
3	陕西省	35	47	76	0.32	111
4	安徽省	40	45	89	0.31	129
5	上海市	22	41	68	0.24	90
6	山东省	27	47	147	0.16	174
7	辽宁省	21	42	128	0.14	149
8	四川省	16	21	115	0.12	131
9	山西省	9	12	87	0.09	96
10	浙江省	9	15	108	0.08	117
11	江苏省	11	14	169	0.06	180
12	黑龙江省	6	7	103	0.06	109
13	湖北省	9	13	135	0.06	144
14	广东省	10	14	162	0.06	172
15	河南省	8	11	144	0.05	152

请各位专家批评指正

谢 谢！

zhangjia@cernet.edu.cn