第三届
全国网络与信息安全防护峰会

对话·交流·合作

XDef 2014

网络攻击再现与攻防过程可视化

陈武平

信息保障技术重点实验室

对话·交流·合作

汇报的主要内容

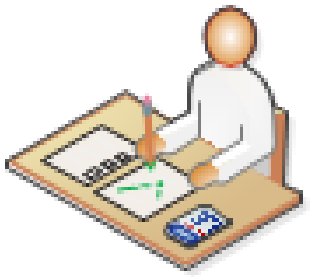
一 问题的提出

二 必要性

三 方案

四 意义

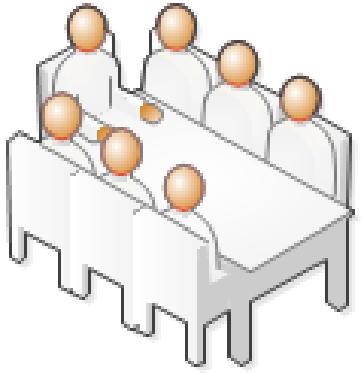
一、问题的提出



在构建一个网络系统安全解决方案时，技术人员会根据网络的拓扑结构、网络运行的业务、网络使用人员、网络的使用环境以及用户的重点关注等，提出整体的安全防护策略和解决方案。这个方案的每一个策略，可能都面对着一种或多种安全威胁，但是一般只是在方案的需求部分进行文字的描述。

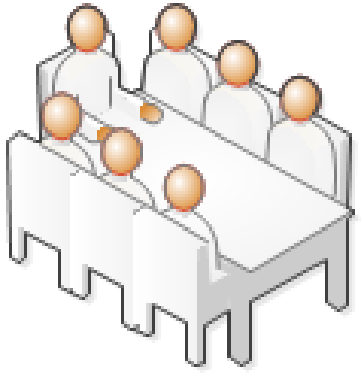
一、问题的提出

但是从决策者的角度，对于这些安全威胁是否存在、会造成什么后果，该方案是否反应过度等，都会产生不同程度的疑虑，严重的甚至不能说服决策者做出正确的抉择。



一、问题的提出

出现这种问题的情况应该说比较普遍。究其原因，主要是在网络这个虚拟世界中，决策者没有直观地看到过这些网络攻击威胁确实存在、确实会造成严重后果，于是提出了网络攻击行为再现工程和网络攻防过程的可视化问题。



一、问题的提出

网络攻击再现是为了直观反映攻击行为存在的客观性和后果的危害性；

攻防过程可视化是为了客观反映防御措施的有效性。

汇报的主要内容

一 问题的提出

二 必要性

三 方案

四 意义

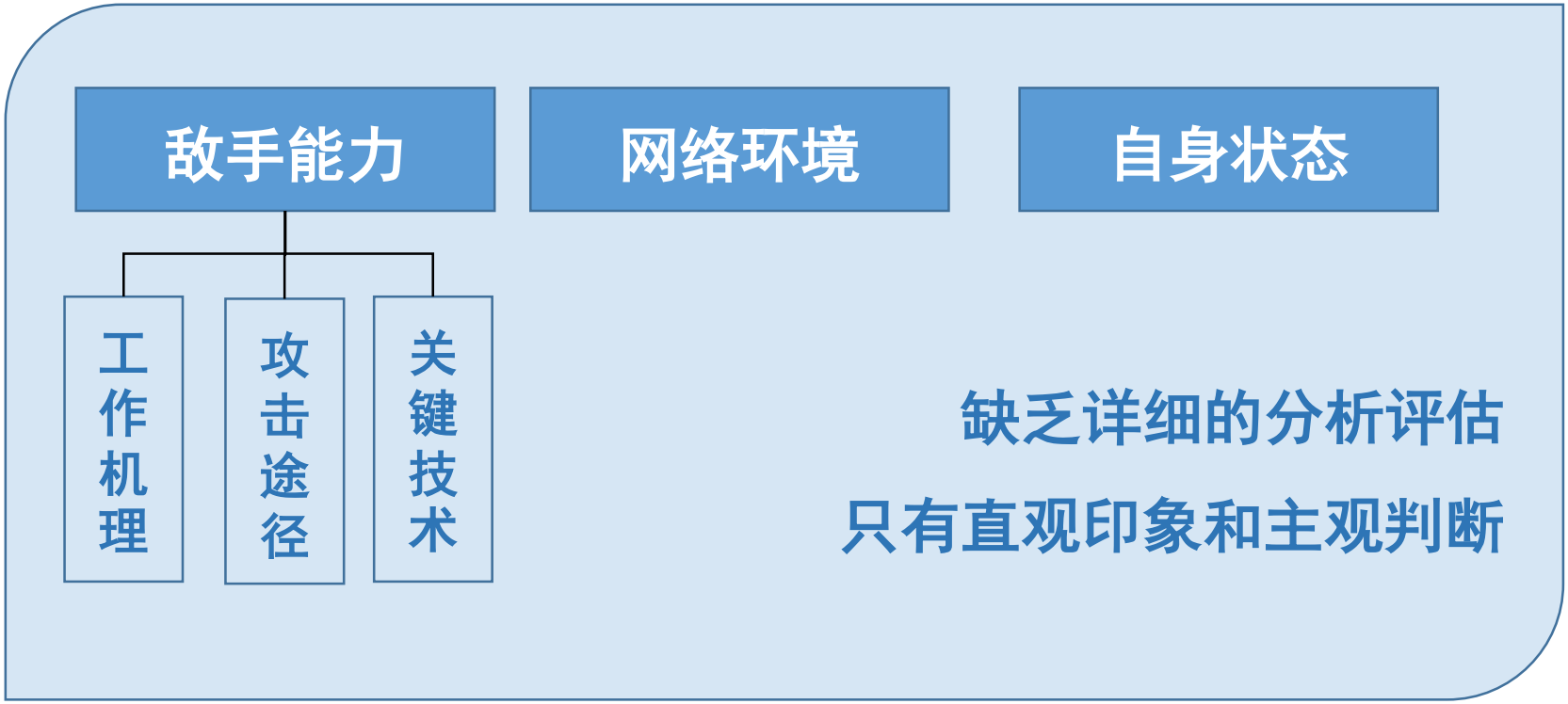
二、必要性

（一）改进安全防护工作方式

目前在做网络安全防护方案时，主要是根据经典的网络安全防护理论，以及多年的实际工作经验，综合采用现有的安全防护手段，构建一整套安全防护体系框架。这种防护方案形成方式有以下缺点：

二、必要性

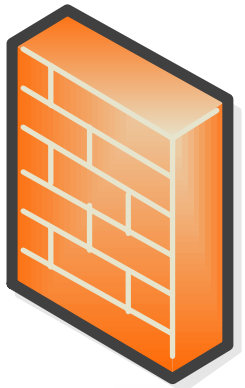
1、安全防护方案的主观性明显



二、必要性

1、安全防护方案的主观性明显

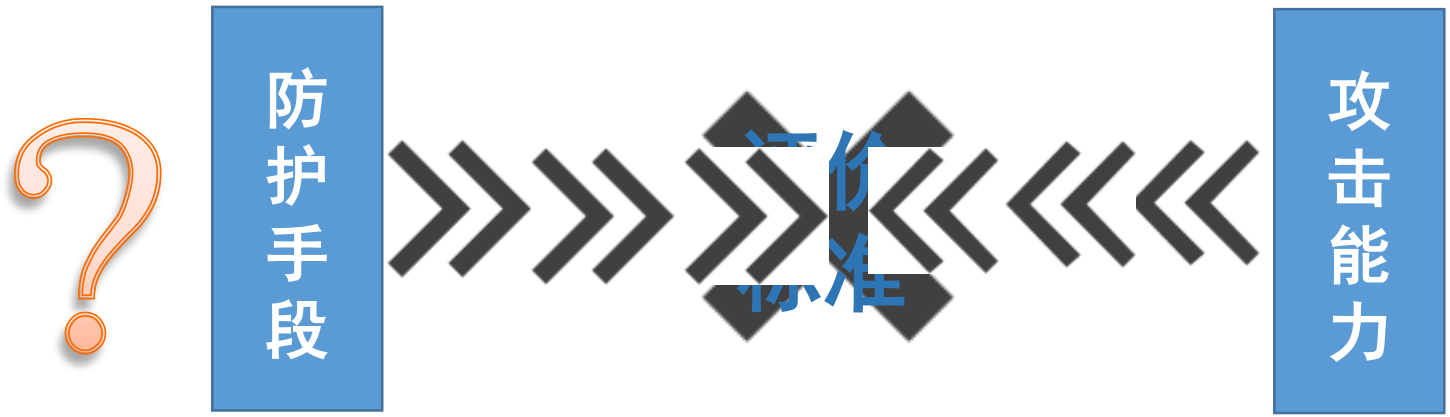
宁多勿缺



- 防护的粒度较粗
- 针对性较差
- 影响系统的工作效率

二、必要性

2、不能为决策者和使用者，甚至是设计者释疑



- 是否需要这样的防护方案？
- 是否经得起APT等高级手段的攻击？

二、必要性

（二）促进APT攻击的复现和还原

	1	2	3	4	5	6	7	8	9	10	11
	锁定目标	组建队伍	构建或购买工具	研究目标	针对检测测试	部署实施	初始入侵	出局连接	建立立足点	盗取数据	掩藏踪迹持续渗透
黑客行动主义	■	■	■			■	■	■		■	
网络犯罪			■		■	■	■	■		■	
APT攻击	■	■	■	■	■	■	■	■	■	■	■

二、必要性

（二）促进APT攻击的复现和还原

54%

的恶意软件，传统AV无法检测

NTT Group《2014 Global Threat Intelligence Report》

87%

数据泄露事件，传统检测技术无法发现

Verizon：《2013 Data Breach Investigations Report》

二、必要性

（二）促进APT攻击的复现和还原

一种可行的方法是以攻击目标为起点，以攻击源为终点，以攻击后果为依据，根据网络拓扑以及系统安全状态评估反推出可能的攻击路径及需要采用的技术手段，从而复现和还原APT攻击。

二、必要性

（三）推动网络攻防的可视化和交互的人性化

网络攻防是
一种无硝烟的战争

二、必要性

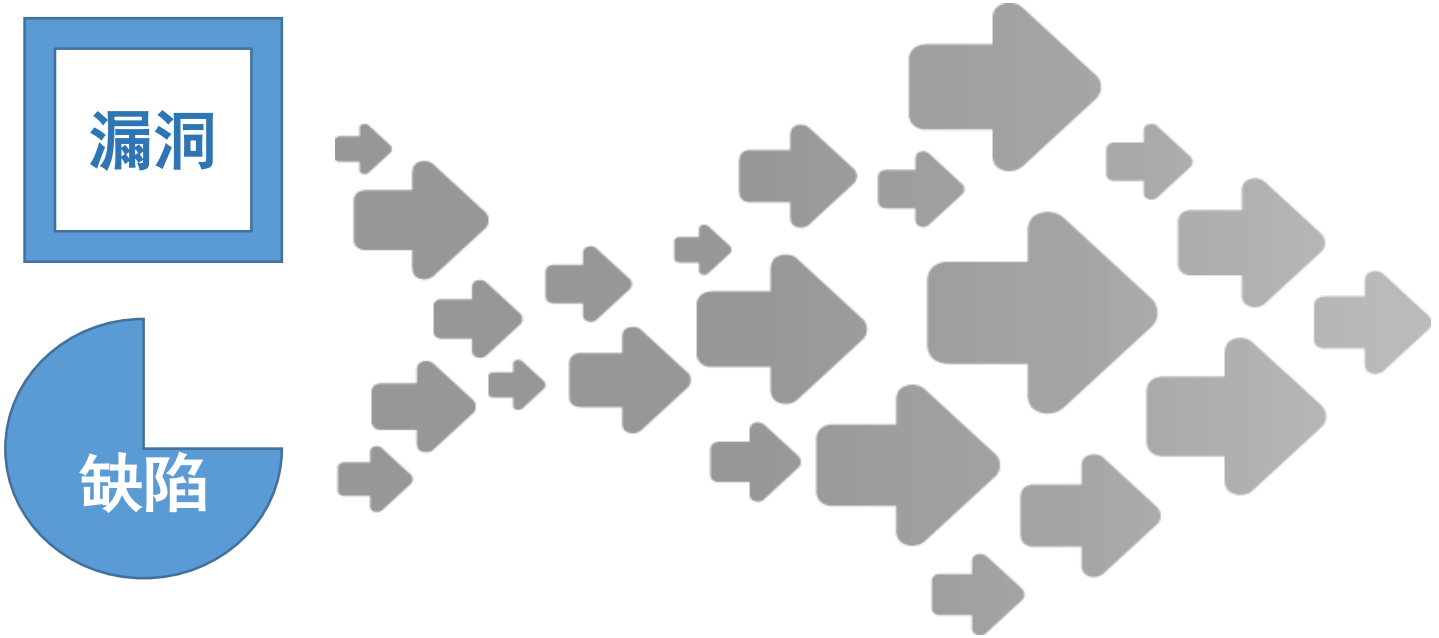
（三）推动网络攻防的可视化和交互的人性化

二、必要性

（三）推动网络攻防的可视化和交互的人性化

因此迫切需要直观和多样的网络攻防可视化手段，为决策者和其他用户提供可视化的演示环境和丰富的人机交互平台。

二、必要性



- 一是使得网络安全防护方案具有很强的针对性和说服力；
- 二是通过网络攻击手段的配置使用和网络攻击的复现还原，使得网络攻防具有更好的展示效果。

汇报的主要内容

一 问题的提出

二 必要性

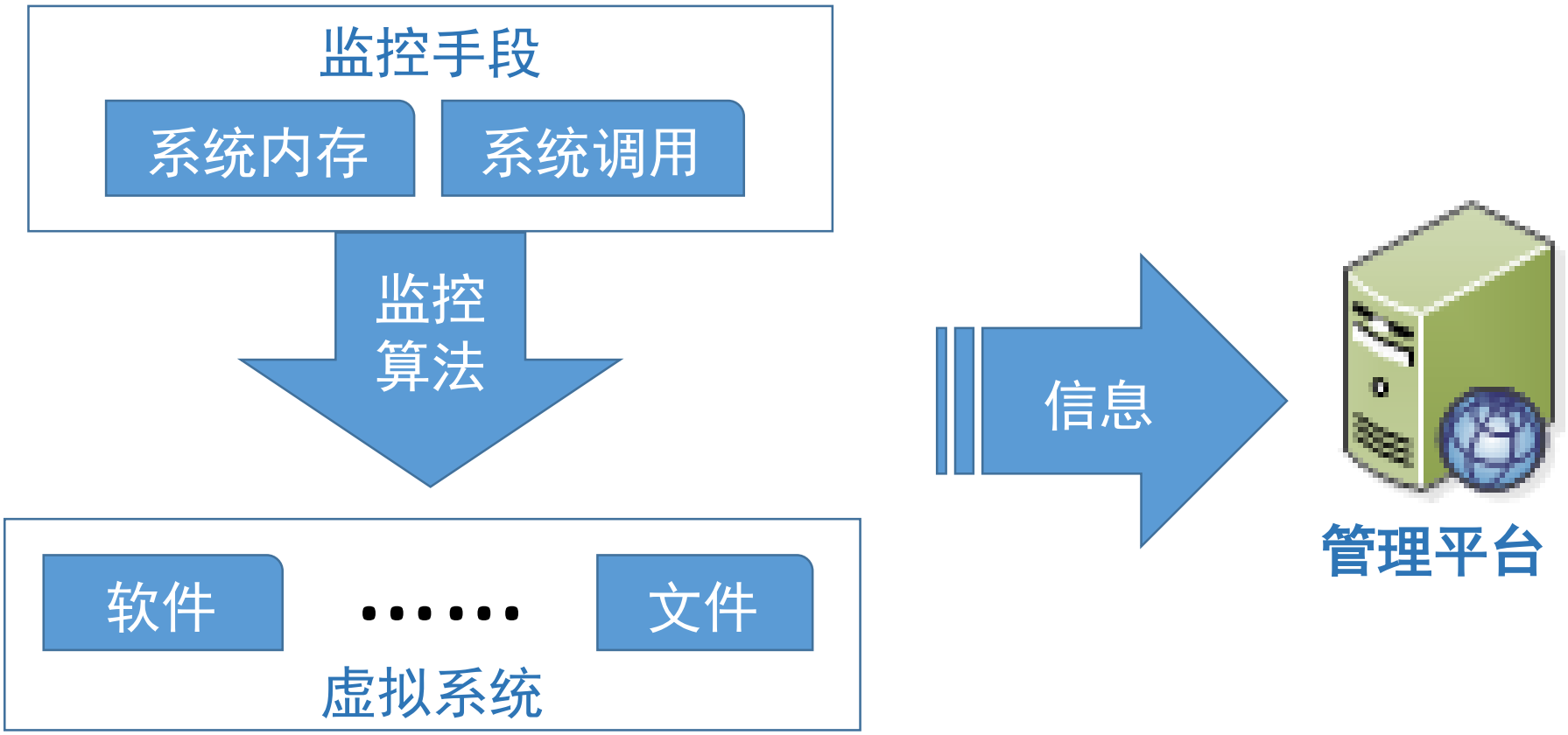
三 方案

四 意义

三、方案

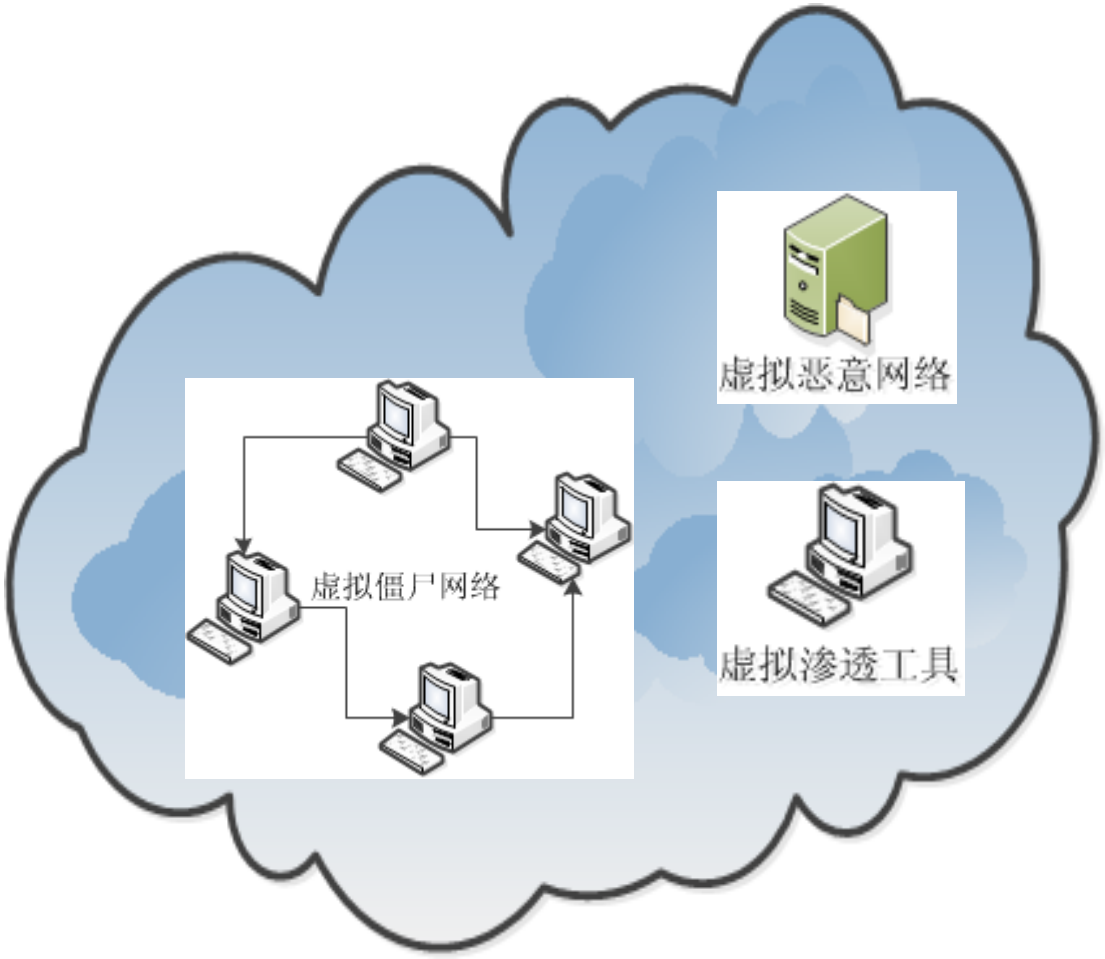
网络攻击再现与攻防过程可视化需要以仿真实验环境为依托。仿真实验环境是一个相对灵活设置、易于实施的、平台开放的、攻击目标明确的虚拟攻击场景。该场景是对真实的网络场景的最大限度的仿真。

三、方案



三、方案

攻击方网络

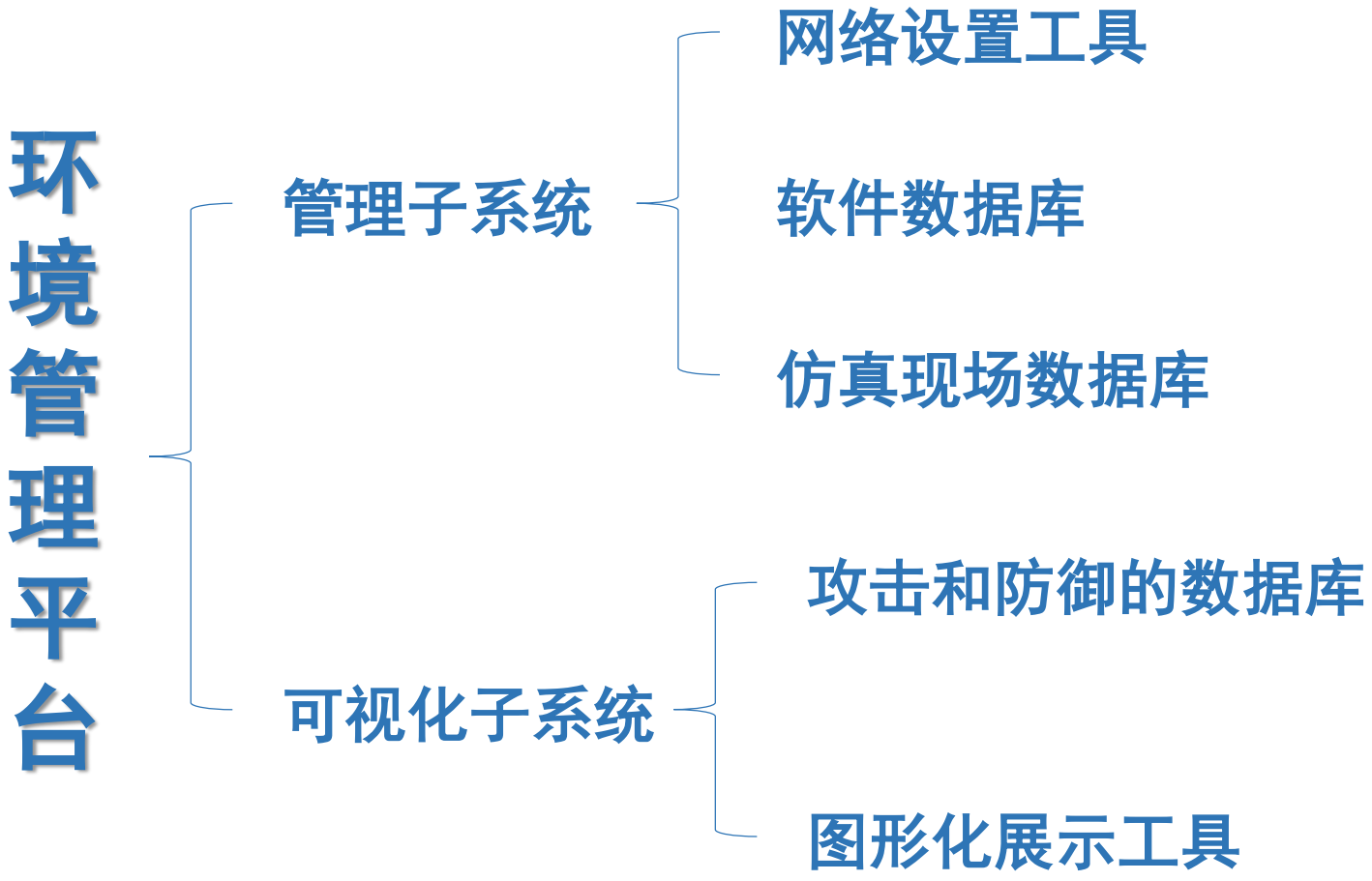


- 渗透工具
- 模糊测试工具
- 植入工具
- ……

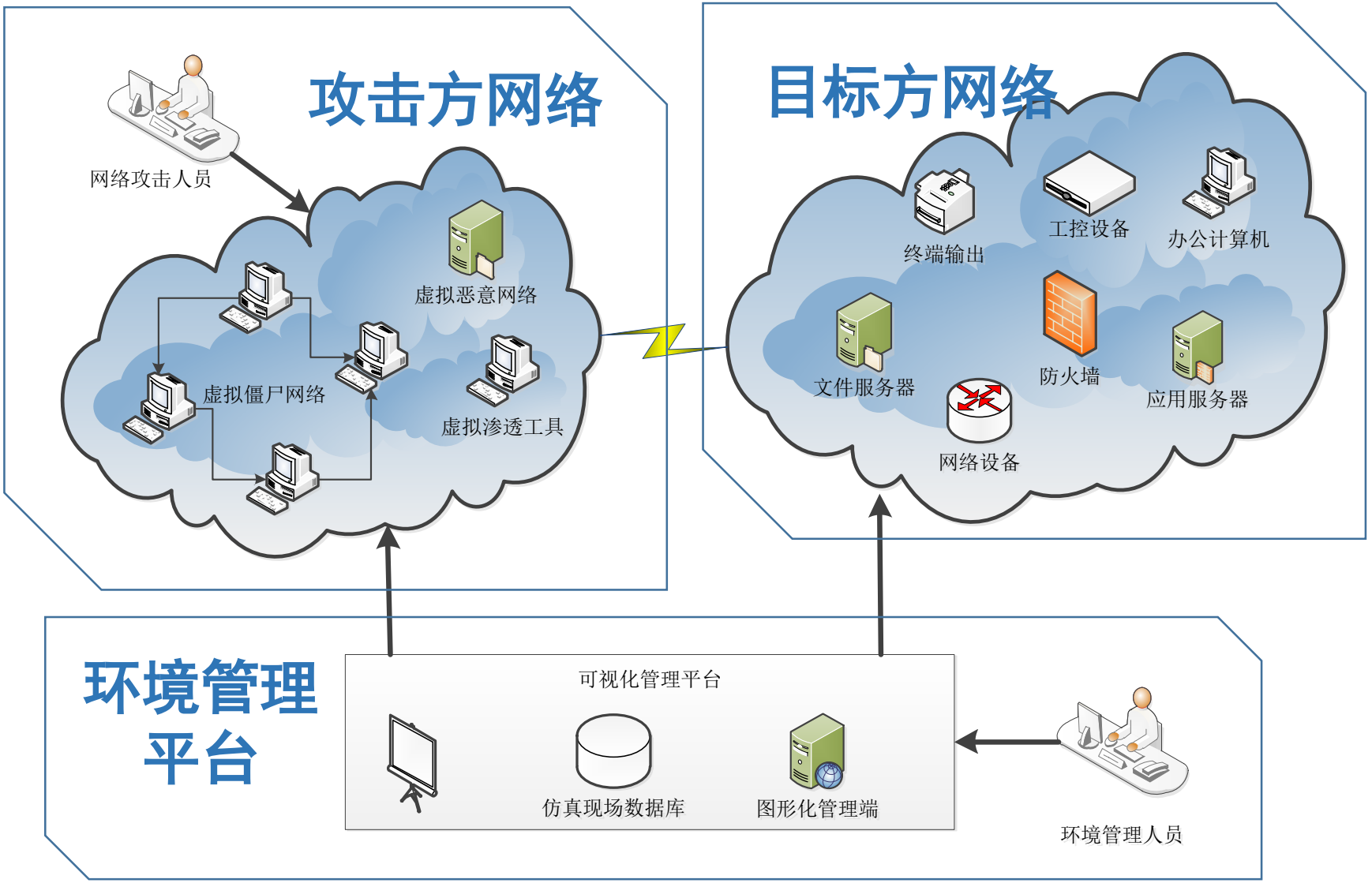
三、方案

目标方网络

三、方案


环境管理平台
管理子系统
网络设置工具
软件数据库
仿真现场数据库
可视化子系统
攻击和防御的数据库
图形化展示工具

三、方案


攻击方网络
网络攻击人员
虚拟恶意网络
虚拟僵尸网络
虚拟渗透工具
目标方网络
终端输出
工控设备
办公计算机
文件服务器
防火墙
应用服务器
网络设备
环境管理平台
可视化管理平台
仿真现场数据库
图形化管理端
环境管理人员

三、方案

通过该实验环境可以恢复各种已知和未知的攻击，在恢复的过程中可以找出不同的攻击手段和途径，同时管理方可以一目了然地观察到攻击的时间、方法和效果，为理论研究和防御策略的制定提供有力支撑和有效补充。

汇报的主要内容

一 问题的提出

二 必要性

三 方案

四 意义

四、意义

网络攻击再现与攻防过程可视化不但要进行理论研究，而且需要建立网络攻防演示验证实验环境，进行理论与实践的结合，对网络信息安全的发展有着积极的指导和借鉴作用。

四、意义

一是通过网络攻击再现，恢复各种攻击方法，使人一目了然的看到攻击的过程和效果。

通过网络攻击再现对攻击的整个过程进行还原和模拟，构造出多种有相同效果的攻击方法和途径，并利用实验环境展现整个攻击过程。通过展现整个攻击过程，可以更加直观地发现日常防护过程中的薄弱环节和安全隐患，为完善防护措施，提高防护能力提供依据。

四、意义

二是逆向恢复过程中可能会产生不同的、多种攻击方法和途径，对网络安全防护方法和措施有一个多途径的参考，提高防护水平。

逆向恢复过程中，通过反向思路可以从新的角度对攻击进行分析，不同于以往正向推导的思路，因此，很可能在网络攻击再现过程中发现不同的攻击方法和途径。同时由于模拟实际网络环境接入了大量的网络安全设备等防护手段，因此，在演示过程中也可能发现新的攻击途径和方法。通过网络攻击再现，可以对各种已知和未知攻击有更加全新的认识。

谢　谢