doi:10.11959/j.issn.1000-436x.2017281

网络欺骗技术综述

贾召鹏[1,2]，方滨兴[1,3,4]，刘潮歌[2,5]，刘奇旭[2,5]，林建宝[1,2]

(1. 北京邮电大学网络空间安全学院，北京 100876；2. 中国科学院信息工程研究所，北京 100093；
3. 广州大学网络空间先进技术研究院，广东 广州 510006；4. 电子科技大学广东电子信息工程研究院，广东 东莞 523808；
5. 中国科学院大学网络空间安全学院，北京 100049)

摘 要：网络攻防不对称是当前网络安全面临的核心问题之一。基于欺骗的防御技术是防御方为改变这种不对称格局而引入的一种新思路，其核心思想是通过干扰攻击者的认知以促使攻击者采取有利于防御方的行动，从而记录攻击者的活动与方法、增加其实施攻击的代价、降低其攻击成功的概率。首先，对网络欺骗进行形式化定义并依据欺骗环境构建方法将其划分为 4 种。同时，将网络欺骗的发展历程概括为 3 个阶段，分析各个阶段特点。然后，提出网络欺骗的层次化模型并对已有研究成果进行介绍。最后，对网络欺骗对抗手段进行分析与总结并介绍网络欺骗技术发展趋势。

关键词：网络欺骗；认知；攻击；防御

中图分类号：TP393 **文献标识码**：A

Survey on cyber deception

JIA Zhao-peng[1,2], FANG Bin-xing[1,3,4], LIU Chao-ge[2,5], LIU Qi-xu[2,5], LIN Jian-bao[1,2]

(1. School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
3. Cyberspace Institute of Advanced Technology, Guangdong University, Guangzhou 510006, China;
4. Institute of Electronic and Information Engineering of UESTC in Guangdong, Dongguan 523808, China;
5. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: The asymmetric situation of network attacks and defenses is one of the key issues of current network security. Cyber deception was a revolutionary technology introduced by defenders to alter the asymmetric situation. By thwarting an attacker's cognitive processes, defenders can mislead attackers, hence causing them to take specific actions that aid network security defenses. In this way, defenders can log attackers' behavior and method, increase cost for the attackers to launch a successful attack, as well as reduce the probability of an attacker's success. Cyber deception formally and classify cyber deception into four classes was defined. Then, the cyber deceptions' development was divided into three stages, and each stage's character was decided. Next, a hierarchical model to describe the existing work was proposed. At last, the countermeasures in cyber deception and the development trends in this field was discussed.

Key words: cyber deception, cognitive process, attack, defense

1 引言

网络欺骗是由蜜罐演进而来的一种防御机制。在网络攻击中，攻击一般需要依据网络侦查获取的信息来决定下一步动作，网络欺骗正是利用这一特点，通过干扰攻击者的认知以促使攻击者采取有利

收稿日期：2017-03-27；**修回日期**：2017-08-16
通信作者：刘潮歌，liuchaoge@iie.ac.cn
基金项目：国家重点研发计划基金资助项目(No.2016YFB0801604)；东莞市引进创新科研团队计划基金资助项目(No.201636000100038)；中国科学院网络测评技术重点实验室和网络安全防护技术北京市重点实验室基金资助项目

Foundation Items: The National Key Research and Development Program of China (No.2016YFB0801604), Dongguan Innovative Research Team Program(No.201636000100038), Key Laboratory of Network Assessment Technology at Chinese Academy of Sciences and Beijing Key Laboratory of Network Security and Protection Technology

于防御方的行动。与传统安全技术相比，网络欺骗不是着眼于攻击特征而是攻击者本身，可以扭转攻击者与防御者之间的攻防不对称。

1) 当前网络系统的确定性、静态性和同构性[1, 2]，使攻击者可以通过探测等手段获知目标的信息，对目标系统的脆弱性进行反复的分析和渗透测试，从而找到对应的策略。通过网络欺骗技术可以打破网络系统的确定性、静态性与同构性，使攻击者无法获取准确的环境信息。

2) 一次攻击的失败为攻击者提供了改进的经验，而一次防御的成功对于防御方来说因为看到的是失败的攻击，防御方不能预知攻击方下一步的动作。通过网络欺骗技术将攻击者引入一个“伪造”的环境中，使攻击者无法判断攻击是否成功，同时通过对攻击者攻击活动的记录和分析，防御方可以获取更多攻击者的信息。

3) 对于业务网络中部署的商业化边界防御设备，攻击者可以通过扫描、踩点等手段侦察相关信息，并使用同样的安防产品进行网络武器的验证与测试。网络欺骗技术与业务环境相融合，攻击者探测到的并不是准确的业务环境，也就无法构建同样的环境进行武器实验。

4) 通过在业务系统中布置伪造的数据，即使攻击者成功窃取了数据，也会因为虚假数据的存在而降低了数据的总体价值。

网络欺骗因其自身的优势而受到了安全防御人员的关注。在学术界，2016 年，Springer 出版社出版了《Cyber Deception》[3]，这是第一本专门介绍网络欺骗研究的著作，汇集了最新的网络欺骗相关的研究工作；近年来，CCS、NDSS、USENIX Security 等国际安全会议上也有相关学术论文发表[4~8]。在产业界，从 2014 年起，包括以色列 Illusive Networks、美国 TrapX Security、中国长亭科技、默安科技等多家公司推出了基于欺骗的安全产品来对抗高级威胁；2015 年，Gartner 发布报告，预测到 2018 年将会有 10%的公司采用基于欺骗的策略保护自身安全[9]；2017 年，Markets and Markets 公司发布的报告认为到 2021 年欺骗防御的市场规模将达到 20.9 亿美元。在政府方面，美国海军在 2003 年就有使用网络欺骗应对网络恐怖主义的研究[10]；美国国防高级研究计划署（DARPA, defense advanced research projects agency）也进行了网络欺骗技术的探索[11]；2014 年，美国空军在一份名为《Capabilities for Cyber Resiliency》的文件中提到要研究网络欺骗技术用于网络空间对抗。

国内学者很早就对网络欺骗初期技术进行了研究，2002 年中国科学院高能物理研究所刘宝旭等[12, 13]就进行了陷阱网络的探索，诸葛建伟等创建了“狩猎女神”项目组并积极开展蜜罐研究工作。然而之前网络欺骗技术综述工作都偏重于对蜜罐技术的介绍[13~16]，不能清楚地描绘出网络欺骗技术的含义。本文贡献如下。

1) 结合已有文献对网络欺骗技术的描述给出网络欺骗的形式化定义，并从欺骗环境构建的角度将网络欺骗分为 4 种。

2) 根据网络欺骗应对目标的不同，将网络欺骗技术的发展分为 3 个阶段，分别总结每个阶段的特点和代表性工作。

3) 从网络欺骗作用点的角度提出网络欺骗层次模型，并对已有研究进行分类介绍；结合入侵杀伤链分析不同研究在杀伤链各个阶段的作用。

4) 将现有网络欺骗对抗技术分为 3 种，并阐述反对抗机制。

2　网络欺骗形式化定义

2.1　定义

网络欺骗是欺骗策略在网络安全防御中的应用。Whaley 认为欺骗是一种认知的形式，通过另外一个人的活动故意导致目标不正确的认知，欺骗有别于自欺，同时欺骗含有故意的因素，无意识的描述错误不属于欺骗[17]。图 1 展示了 Whaley 对认知的分类。

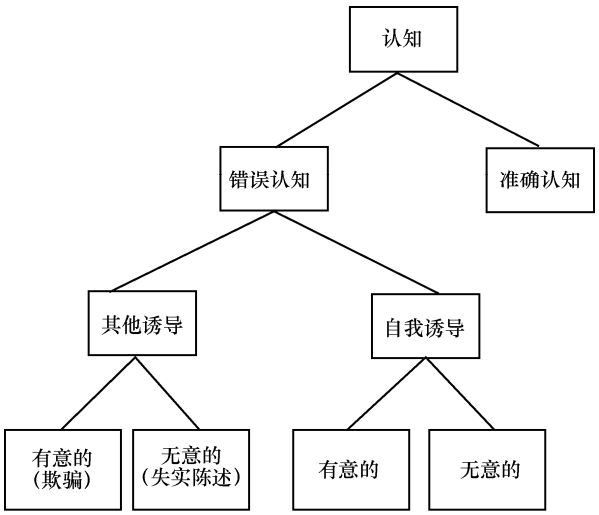


图 1　认知分类

军事上欺骗被定义为蓄意误导敌方军事决策者，使之对己方能力、意图和行动误判，从而导致对手采取有助于己方完成任务的具体行动（或不行动）[18]。这一定义中也突出了蓄意误导以使目标产生误判。在参考这一定义的基础上，Yuill[19]给出了计算机安全欺骗（computer-security deception）的定义为了误导攻击者而采取的有计划的行动，使攻击者采取（或不采取）特定的行动以增加计算机安全防御。Almeshekah 等[20]在 Yuill 定义的基础上在目的中加入了“扰乱”，定义欺骗是为了误导和/或扰乱攻击者的有计划的行动，以让攻击者采取（或不采取）特定的动作来增加计算机安全防御。

Gartner 对欺骗技术的描述为欺骗技术被定义为使用骗局或假动作来阻挠或推翻攻击者的认知过程，扰乱攻击者的自动化工具，延迟或阻断攻击者的活动，通过使用虚假的响应、有意的混淆以及假动作、误导等伪造信息达到“欺骗”的目的。

通过上述描述可以看出，欺骗是有意地误导对手的决策从而使对手以有利用于防御方的形式行动或者不行动。在对此类技术的描述上有的文献称为“欺骗（deception）”，有的称为“计算机安全欺骗（computer-security deception）”，这些都不够准确，在本文中采用“网络欺骗”来描述此类技术并综合上述定义给出如下描述。

定义 1 网络欺骗（cyber deception）。安全防御人员在己方信息通信系统中布设骗局，干扰、误导攻击者对己方信息通信系统的认知，使攻击者采取对防御方有利的动作(或不行动)，从而有助于发现、延迟或阻断攻击者的活动，达到增加信息通信系统安全的目的。

在上述定义的基础上给出网络欺骗的形式化定义，*Cyber-Deception*=(*Defender*, *Asset*, *Trick*, *Attacker*, *Profit*)。

1) *Defender*。安全防御人员，欺骗行动的发起者和实施者，通过策划和实施欺骗以使攻击者采取防御者预期的行动。

2）*Asset*。己方信息通信系统中的资产，网络欺骗要保护的目标。*Asset*=（$asset_1$, $asset_2$,…, $asset_n$），$asset_i$ 为信息通信系统中的设备、系统、软件、应用、数据等。

3) *Trick*。构建的骗局，部署在信息通信系统中。骗局有 2 种，一种是构建虚假资产，记为 *Simulation*；另外一种是对系统中已有资产的特征进行修改，记为 *Modification*，则有 *Trick*=（*Simulation*, *Modification*）。其中，*Simulation*={$sasset_1$, $sasset_2$, …, $sasset_p$}，*Mimulation* ={$masset_1$, $masset_2$,…, $masset_q$}（$p+q>0$, $q\leqslant n$）。对于每个 $masset_i$ 对应 *Assets* 中的 $asset_j$（$i!=j$），对攻击者来说却表现出 $asset_i$ 的特性，使攻击者认为资源看到的是资源 $asset_i$。

4) *Attacker*。攻击者，网络欺骗针对的对象。记为 *Attacker*=(*Tactics*, *Techniques*, *Procedures*)。*Tactic*、*Technique*、*Procedures* 分别表示攻击者使用的手段、技术与过程。网络欺骗设计的过程中要根据攻击者特征采取不同的方案。

5) *Profit*。网络欺骗的收益，也是防御方实施欺骗的目的，记为 *Profit*={*TTP*, *Trace*, *Protection*, *Delay*}。其中，*TTP* 代表通过网络欺骗获取到的攻击者的 *Tactics*、*Techniques*、*Procedures* 信息。*Trace* 代表对攻击者追踪溯源。*Protection* 代表对真实资产的保护。*Delay* 代表对攻击者攻击活动的延迟。

2.2 网络欺骗的安全属性

在网络欺骗中要考虑 4 个属性，即（CACA，confidentiality 、 authentication 、 controllability 、 availability），如图 2 所示。对攻击者而言要有机密性（confidentiality），设计的骗局不可被攻击者识破，一旦被识破也就失去了价值；对防御者而言要有可鉴别性（authentication），设计的骗局对于防御者来说是可鉴别的，防御者能够区分骗局和真实的业务系统；对于用户来说具有可用性（availability），骗局的部署不能影响正常用户的使用与业务系统的正常功能；欺骗系统自身具有可控性（controllability），骗局是可控的，不能被攻击者用做攻击跳板，同时可以观测到攻击者的活动。

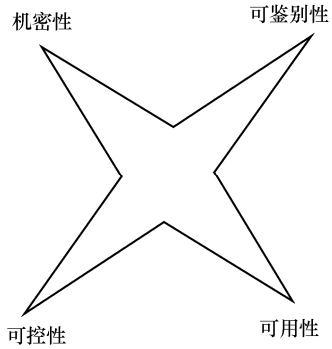


图 2 网络欺骗安全属性模型

2.3　网络欺骗的生命周期

网络欺骗是伴随实际攻防对抗不断变化的，本文将网络欺骗从策划到终止划分为准备（planning）态、闲置（idle）态、工作（working）态、衰弱（failing）态、终止（stopping）态这 5 个状态，状态迁移变化如图 3 所示。

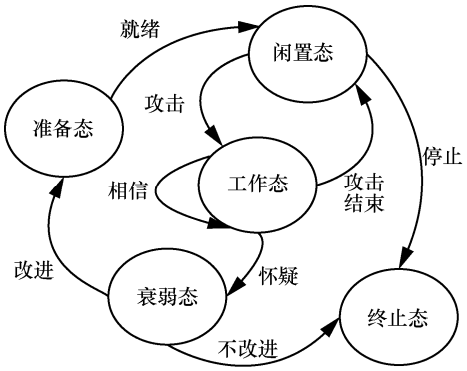


图 3　网络欺骗生命周期

1) 网络欺骗规划设计阶段处于准备态。

2) 当网络欺骗规划完成后，则进入实际部署，此时还没有攻击者步入骗局，进入闲置态。

3) 当有攻击者发起攻击并步入骗局时，网络欺骗进入工作态，当攻击者的攻击结束则网络欺骗变为闲置态。

4) 如果在欺骗过程中攻击者相信了骗局，攻击者就会持续被欺骗，从而网络欺骗一直处于工作态；如果攻击者对欺骗环境产生怀疑，则证明欺骗策略需要调整，网络欺骗进入衰弱态，此时如果对欺骗策略进行改进则网络欺骗进入准备态，如果不对欺骗策略进行改进那么骗局会被攻击者进一步识别从而失去作用，网络欺骗进入终止态。

5) 进入终止态有 2 种方式，欺骗停止和正常终止；骗局被攻击者怀疑后没有改进，从而被动终止。

2.4　分类方法

网络欺骗本质是通过布设骗局从而干扰攻击者认知过程，欺骗环境的构建机制是其实施的关键。本文从欺骗环境构建的角度讨论网络欺骗技术的分类，这也是大多数网络欺骗研究采用的分类方式。蜜罐技术中一般根据欺骗环境提供的交互程度将其分为低交互蜜罐与高交互蜜罐。低交互蜜罐往往采用软件模拟的方式实现，而高交互蜜罐则采用真实系统构建。然而，蜜罐技术仅仅是网络欺骗技术的一种，这一分类方法并不适用于所有的网络欺骗技术，如操作系统（OS, operating system）混淆、蜜标、伪蜜罐等。另外一种使用比较广的方法是 Whaley 建立的欺骗分类[17]，如表 1 所示，将欺骗分为“掩饰”和“模拟”2 种，并分别给出了实现 2 种欺骗的 3 种策略。“掩饰”是通过掩盖目标的特征来避免对手发现真相，“模拟”则是通过假装或描绘假的东西，使受骗者认为观察的假象是真的。这一分类的问题是各个策略之间存在交叉，缺乏唯一性描述，如高交互蜜罐同时具有“编造”与“诱骗”2 种策略。本文按照欺骗环境的构建方式将网络欺骗分为 4 种：掩盖、混淆、伪造、模仿。

表 1　　欺骗分类

欺骗类别	策略	定义
掩饰	掩盖	隐藏所有鲜明的特征，或将其与周围的特征相匹配
	重新包装	添加或削减特性而将其转换为其他对象
	目眩	创造全新的或不同的对象
模拟	模仿	复制一个或多个特征来近似某一对象
	编造	随机或部分模糊对象的特性
	诱骗	创造虚假的特性，来给定额外的模式

掩盖欺骗通过消除特征来隐藏真实的资源，防止被攻击者发现。典型工作如网络地址变换，通过周期性重新映射网络地址和系统之间的绑定改变组织网络的外形。Antonatos 等[21]使用动态主机配置协议（DHCP, dynamic host configuration protocol）给每个主机重新分配网络地址，用来对抗带有目标列表的蠕虫。MUTE（mutable networks）使用随机地址跳变技术为主机重分配与真实 IP 地址相独立的随机虚拟 IP 地址，以限制攻击者扫描、发现、识别和定位网络目标的能力[22]。

混淆欺骗通过更改系统资源的特征使系统资源看上去像另外的资源，从而挫败攻击者的攻击企图。典型工作如伪蜜罐[23]，通过使真实系统具有蜜罐的特征从而吓退攻击者。而通过采用计算机操作系统混淆，使受保护的操作系统对远程探测工具表现出其他操作系统的特性，可以挫败攻击者的探测企图[24]。

伪造欺骗通过采用真实系统或者资源构建欺骗环境，通过伪造的资源吸引攻击者的注意力从而发现攻击或浪费攻击者的时间。典型的工作就是高交互蜜罐以及蜜标技术，如蜜网[25]、Honeybow[26]、Honeyfile[27]等。此类技术特点是机密性好，但是维护与部署代价较高。

模拟欺骗则是采用软件实现的方式构造出资

源的特征。典型工作如 deception Toolkit (DTK)[28]，绑定系统未使用的端口从而发现攻击。此类欺骗机密性较低，适用于攻击检测与恶意代码收集，不适合对攻击者行为的长期观察。但是，因为所占资源小而且几乎不会带来风险，因此，可以部署于业务主机之上，检测范围大、使用灵活。

2.5 网络欺骗流程

网络欺骗的设计与实施是一个复杂的过程，因欺骗目的、部署环境、欺骗目标的不同而不同。但是总体来说可以分为设计、实施、评估 3 个过程，一次成功的欺骗往往是 3 个过程不断重复，图 4 展示了网络欺骗基本流程。

1) 欺骗行动设计

在欺骗行动设计阶段，首先，进行需求分析，明确欺骗的目标和目的，以及欺骗活动可能带来的风险及如何控制。针对勒索软件、蠕虫、网络间谍等攻击需要采取的应对措施与要达到的欺骗目的不同，在对目标和目的分析的基础上明确欺骗内容和实施时机。

其次，构建欺骗方案，采用的欺骗方案要与部署的业务环境具有一致性，以防止被攻击者发现。然后选择欺骗组件，确定欺骗策略，如部署虚假操作系统或服务、改变业务系统外在状态等；明确信息通道，即如何使攻击者获得骗局信息从而进入骗局；明确能够观测和评估目标反应的反馈渠道。最后明确欺骗终止条件。

最后，分析攻击者采取的行动、可能出现的问题与响应以及如何与其他防御系统（如 IDS 设备）进行协调等。

2) 欺骗实施

根据欺骗的目标和目的，网络欺骗系统可以部署在业务系统的不同位置。在网关处将业务系统不使用的 IP 与端口指向构建的虚拟环境，可以发现攻击与保护业务系统；在业务系统内部放置诱饵可以发现窃密攻击与勒索软件攻击；通过在真实业务主机中设置虚假的访问记录或访问凭证可以引诱攻击者攻击诱饵服务从而暴露攻击者；将业务系统伪装成虚拟机或蜜罐可以吓退攻击者。

此外还可以通过操作系统混淆技术干扰攻击者信息搜集（如使 Window 系统表现出 Linux 系统

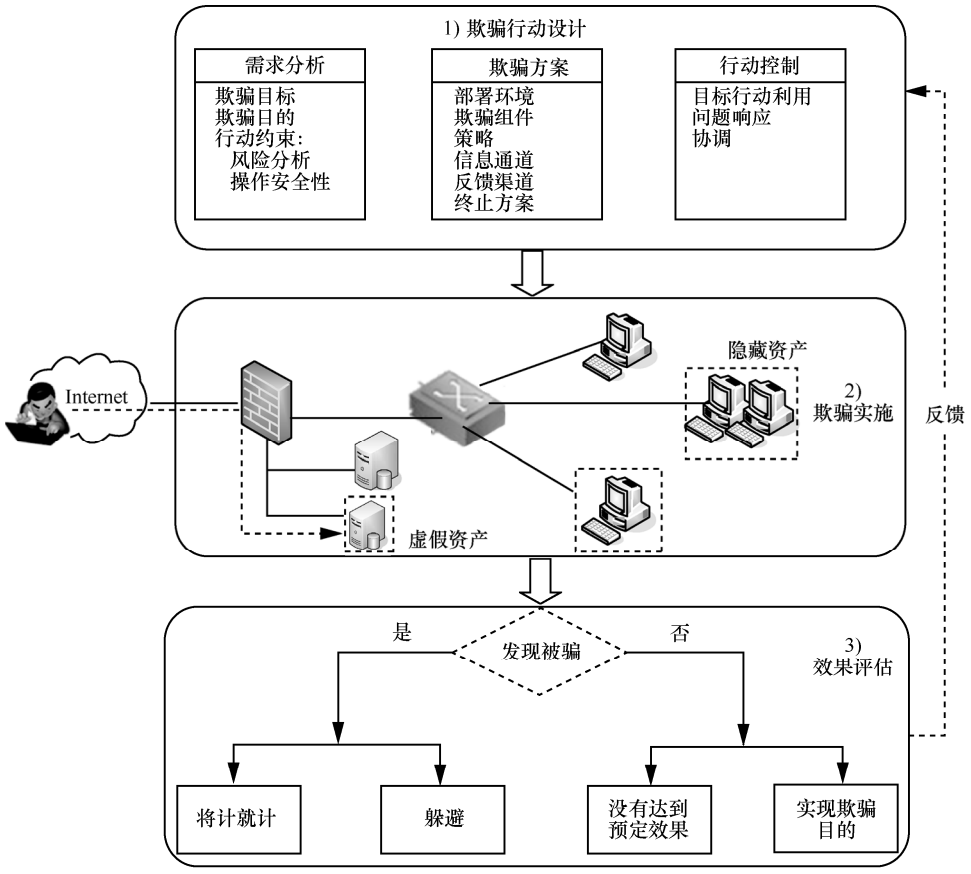


图 4 网络欺骗流程

的特性），或通过网络地址转换技术隐藏业务系统。

网络欺骗系统及采用的欺骗策略根据针对的攻击者的不同而不同。对于低级攻击者，可以采用软件模拟的方式实现诱饵系统，而对于技术高超的黑客为了达到浪费攻击者时间的目的需要提供业务网络模拟，从而使攻击者在模拟环境中浪费时间。

3) 效果评估

欺骗者如果相信了骗局会有 2 种结果，一种是欺骗者被骗，另外，则是因为欺骗强度较小而没有达到预期的效果，此时，防御人员需要根据观测到的结果评估欺骗的效果以改善欺骗计划。如果欺骗对象识别出了骗局，会采取 2 种动作，第一种是采取躲避行为以避开欺骗系统，第二种是假装被欺骗从而反过来欺骗防御者。需要根据评估的结果来调整与完善网络欺骗方案。

3　网络欺骗发展历程

网络欺骗技术的发展历程可以概括为 3 个阶段：应对人工攻击的开创阶段；应对自动化攻击的蜜罐阶段；应对高级持续性威胁（APT, advanced persistent threat）的欺骗防御阶段。

3.1　开创阶段

网络欺骗技术的起源可以追溯到20世纪80年代末期 Cliff Stoll 的书《The Cucko's Egg》中描述的工作[29]，书中介绍了一起跨国网络间谍案的追踪过程，作者在被入侵的系统上伪造了账户和“战略防御计划网络”文件，以此吸引入侵者的注意，为追踪入侵者赢得了时间。1992 年，AT&T 贝尔实验的 Cheswick 在一篇文章中讨论了如何用虚假的信息诱惑黑客[30]，以追踪该黑客和了解其技术。由此可见，网络欺骗技术早期主要是为了对抗人工攻击。

1994 年，Kim 和 Spafford 在介绍 Tripwire 时建议使用植入的文档来检测入侵者[31]，正常的用户不会去访问这些植入的文档，因此，当这些文档被访问时就意味着很可能发生了入侵。

1998 年，第一款采用欺骗技术进行计算机防御的开源工具 DTK 发布[28, 32]。DTK 使用 Perl 脚本实现，绑定系统上未使用的端口，接收攻击者的输入并给出存在漏洞的响应。DTK 不会被攻陷，因而可以部署在实际的业务系统中，使攻击者在入侵系统时需要做更多的选择，以此提前发现攻击和浪费攻击者的时间。

到 20 世纪 90 年代末期，蜜罐的思路开始形成。其定义为一类安全资源，价值在于未授权的利用[33]。其原理是通过布设没有真实业务的系统形成欺骗环境从而诱使攻击者进行攻击。1999 年，Spitzner 创建了蜜网组织（honeynet project），并提出了蜜网的思路。蜜网[33]通过构建一个高度可控的网络，在其中部署真实的系统形成诱骗环境。因为蜜网中采用了真实环境，从而可以捕获丰富的入侵信息。但是蜜网维护代价高，对使用人员专业技能有要求，且相比于 DTK，蜜网需要和真实业务系统相隔离，使蜜网监控范围小，因此多用于研究目的。

这一时期互联网与计算机的应用主要在政府、军队和高校等科研机构，以数据共享为主。网络入侵的攻击者多由专业技术人员手工发起，以窃取数据为目标，网络攻击范围有限。网络欺骗技术仅仅被部分安全管理人员部署在业务系统中用于检测入侵，主要形式是在业务系统中插入虚假数据或开启虚假服务。为了防止这一思路暴露后引起攻击者的警觉，部分安全人员尽管采用了网络欺骗技术，却没有公开描述。

3.2　蜜罐阶段

21 世纪初期左右，蠕虫成为互联网上的主要威胁之一。例如，1999 爆发的“梅利莎”(Melissa)蠕虫、2000 年爆发的“爱虫”（I Love You）蠕虫、2001 年爆发的“红色代码”（Code Red）蠕虫、“尼达姆”（Nimda）蠕虫、2003 年爆发的 SQL Slammer 蠕虫等。蠕虫可以通过共享文件夹、电子邮件、系统漏洞等方式进行传播，互联网的发展使蠕虫可以在极短时间内蔓延全球，蠕虫的早期检测对蠕虫的防范至关重要。

蜜罐因为捕获数据价值高、几乎没有误报、能够检测 0 day 攻击，且只要蜜罐系统能够覆盖网络的一小部分 IP 地址，就可以在早期检测到蠕虫的爆发，因此受到重视。David 等[34]提出了 HoneyStat 系统，针对局域网蠕虫传播的场景，通过对网络活动、磁盘写、内存操作 3 个方面进行监测，能够在爆发初期检测蠕虫。Crandall 等[35]针对数据劫持漏洞蠕虫提出一种蜜罐检测架构。Honeycomb[36]实现了利用蜜罐进行攻击特征提取,自动产生入侵检测系统签名。Schryen 等[37,38]用电子邮件蜜罐研究利用电子邮件传播的蠕虫。

随着恶意网页威胁的增大，2006 年第一款客户端蜜罐 HoneyMonkey 出现[39]，使用存在漏洞的系统模拟人的操作与网站交互，从而发现恶意网站。

随着新恶意代码产生率的增高，迫切需要自动

化的方式来采集恶意代码。Baecher 等[40]提出了 Nepenthes 解决方案，通过模拟网络服务漏洞从而收集利用这些漏洞进行传播的恶意代码。这一方案的优点是便于大规模部署，然而对利用新漏洞进行传播的恶意代码应对能力不足。诸葛建伟等[26]提出了 HoneyBow 方案，采用真实系统构建恶意代码捕获器，从而可以捕获未知恶意代码，但是因为采用了真实系统进行部署，所以部署成本较高。

随着各种网络应用及非 PC 设备进行传播的恶意代码增多，也出现了相应的蜜罐，如 Web 应用蜜罐、SSH 应用蜜罐、SCADA 蜜罐、VoIP 蜜罐、蓝牙蜜罐、USB 蜜罐、电话蜜罐、数据库蜜罐等。

在这一时期，自动化传播的恶意代码成为主流攻击方式，恶意代码的发现与样本收集的实际需求促进了蜜罐技术的发展。

3.3 欺骗防御阶段

2011 年以后，随着高危软件漏洞的减少和网络运营商大规模封锁高危端口（如 TCP 135/445），蠕虫生存环境急剧恶化，致使蠕虫趋冷，蜜罐技术研究也随之趋缓。其后，高级持续性威胁出现，传统安全机制无法很好地应对此类威胁，安全研究人员再次将目光转向网络欺骗技术，网络欺骗思想开始成熟。一些新兴的安全公司发布了一系列基于欺骗的安全防御产品，网络欺骗技术再次成为安全人员关注的焦点，表 2 列出了部分安全公司的网络欺骗产品及融资时间。

蜜罐是网络欺骗的一种，主要通过布设虚假资源来引诱攻击者采取行动，从而发现攻击与收集攻击信息。从发展历程来看，现有蜜罐技术主要是针对具有大规模影响范围的非定向攻击。定向攻击强调对少数特定目标进行感染和控制，隐蔽性强。因此，仅在未用网段上部署蜜罐系统的部署方式限制了其监控的效率，需要其他欺骗手段进行配合；蜜罐环境尚无法有效解决仿真度与可控性之间的矛盾[16]，且在部署中往往没有真实的业务，欺骗的层次较低，使蜜罐很容易被攻击者识别。现有蜜罐技术的不足使其在应对定向攻击中存在不足。

网络欺骗技术利用攻击者需要依赖探测到的信息以决定下一步动作这一特点，通过构造一系列虚假信息误导攻击者的判断，使攻击者做出错误的动作。除了蜜罐技术外，网络欺骗还包括对真实资源进行伪装，这是一种积极主动的防御策略；网络欺骗技术即可以单独使用，也可以部署于业务系统之上，还可与已有的网络防御机制（如防火墙、IDS、IPS 等）联动，提高系统识别威胁和应急响应的能力；定向攻击持续时间长，为了达到让攻击者在“骗局”中持续攻击的目的，需要模拟出业务网络，这需要网络拓扑仿真等虚拟化技术。网络欺骗包含蜜罐技术、蜜标、网络流量仿真、网络地址转换、拓扑仿真、系统混淆等，图 5 展示了蜜罐与网络欺骗技术的关系。

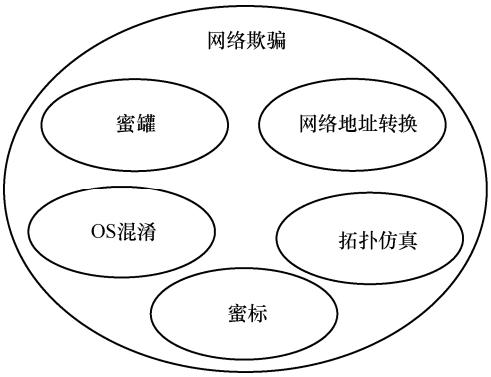


图 5 网络欺骗与蜜罐关系

表 2 部分安全公司产品及融资情况

公司	国家	产品/方案	防御功能	融资情况
Illusive Networks	以色列	Deceptions Everywhere®	伪装欺骗	2015 年 6 月获得 500 万美元融资 2015 年 10 月获得 2 200 万美元融资
Cymmetria	以色列	MazeRunner	伪装欺骗	2015 年累计获得 1 050 万美元融资
TrapX	美国	DeceptionGrid Platform	伪装欺骗	2014 年 1 月获得 500 万美元融资 2015 年 7 月获得 900 万美元融资
Attivo	美国	ThreatMatrix Platform	伪装欺骗	2015 年 4 月获得 800 万美元融资
Allure	美国	Novo Platform	伪装欺骗	——
长亭科技	中国	谛听威胁感知系统	伪装欺骗	2015 年 9 月获得 600 万元天使轮投资
默安科技	中国	幻盾	伪装欺骗	2017 年获得 3 000 万元投资

4　网络欺骗层次化模型

根据网络欺骗的作用点可以分为不同的层次，本节提出网络欺骗实施的层次化模型，按作用点的不同分为设备欺骗、网络结构欺骗、数据欺骗、应用欺骗，如图 6 所示，并结合网络杀伤链概念分析在攻击的各个阶段可以采用的网络欺骗技术。

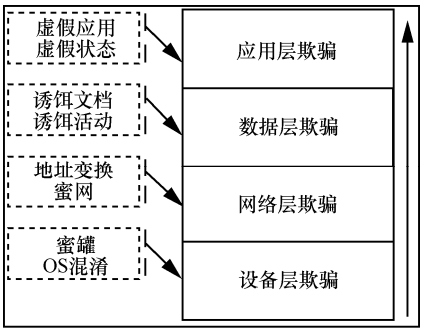


图 6　网络欺骗层次化模型

4.1　设备层欺骗

设备层欺骗通过伪装成有漏洞的终端设备来欺骗攻击者。比较早的实现方式是通过软件模拟的方式进行，如 DTK 欺骗工具[28]，通过绑定系统上空闲的端口，监听攻击者对这些端口的探测并做出存在漏洞的响应，使攻击者认为发现了存在漏洞的系统。类似研究工作还有 Nepenthes 蜜罐[40]和 Dionaea 蜜罐，这 2 种蜜罐主要用于收集恶意软件。

采用此类方式实现的欺骗其交互程度有限，易于被发现。为了使欺骗环境能够提供更多的交互，可以采用真实系统来构建欺骗环境，此类系统的难点在于系统活动的记录和风险的控制，关注点一般在监控工具的开发上。如 HoneyBow 组件，可以安装在用作诱饵的虚拟机系统及宿主操作系统上，通过文件系统监控和交叉对比方法自动获取感染诱饵系统的恶意代码[26]。Argos 蜜罐[41]基于开源 x86 虚拟机 Qemu 构建，在 Qemu 模拟机制上实现了检测记录机制，通过扩展动态污点分析(extended dynamic taint analysis)技术[42]跟踪运行时刻接收到的网络数据，从中识别出非法行为。

除此以外，还可以通过更改设备的特征使攻击者攻击失败或不采取进一步的行动以保护资源。攻击者通常想要规避蜜罐，以避免被发现，在攻击中会采用一些方法来检测当前系统是不是蜜罐[43]，Rowe 等[23,44]利用这一特点通过使业务系统看上去像蜜罐使攻击者不敢访问系统。而通过采用计算机操作系统混淆，使受保护的操作系统对远程探测表现出其他操作系统的特性可以挫败攻击[24]。Zhao 等[45]提出基于软件定义网络（SDN, software defined network）的指纹跳变技术（FPH, fngerprint hopping method），通过监控每个连接的流量以识别出潜在的指纹探测，如果一次通信被检测出有指纹探测行为，那么出口流量就会被重定向并修改其指纹以达到指纹跳变的目的。

随着网络融合时代的来临，安全威胁已经不仅仅限于传统互联网，也向其他领域扩散，为了应对此类威胁，研究人员也采用其他领域的设备来进行欺骗。网络犯罪分子越来越多的使用预录电话（robocalling）、语音钓鱼来欺骗用户。为更好地了解电话威胁以应对此类攻击，Gupta 等[8]使用电话蜜罐来收集电话滥用情报，使用云基础设施和 39 696 个电话号码，在 7 周的时间里收到了 25 万个来源的 130 万个电话，从中检测到了一些电话销售通话和一例电话拒绝服务攻击。针对工控系统的安全问题，趋势科技部署了工控蜜罐，通过模拟 ICS/SCADA 设备，伪装成一座水压力站，仅仅部署 18 h 就捕获到第一例攻击，在 28 天的时间里捕获到了来自 14 个国家的 39 次攻击[46]。

4.2　网络层欺骗

网络层欺骗考虑的是欺骗节点在己方网络中部署的问题以及己方设备的隐藏问题。通过在组织网络中部署设备层欺骗系统以发现攻击或者改变现有设备的网络状态以隐藏资产。网络层欺骗优点是作用范围广，但是为了达到机密性需要设备层欺骗、数据层欺骗和应用层欺骗配合。

Provos 开发的 Honeyd[47]支持构建虚拟网络拓扑结构，并以插件方式提供对各种应用层网络服务的模拟响应，方便进行大范围网络地址的监测。此种方式可以利用很少的资源实现大规模的部署，然而容易被识别且无法提供完整的交互过程。

Spitzner 等[33]提出的蜜网（Honeynet）由防火墙、入侵检测、数据记录、自动报警与数据分析等模块组成控制网络，在其中部署由真实系统构建的蜜罐系统组成蜜罐网络。整个网络通过一个蜜网网关与业务网络相连，蜜网网关不对通过的报文进行 TTL（time to live）递减，以防止被攻击者发现。蜜网结构提供了安全可控的环境来部署作为诱饵的

真实系统，使安全研究人员能够捕获更全面的攻击活动，但是部署真实系统资源消耗与维护代价较高。Artail 等[48]提出了混杂模式的蜜罐架构，使用低交互蜜罐在空闲的 IP 上模拟操作系统与服务，而将收到的恶意流量引至高交互式蜜罐，兼顾了检测范围和欺骗真实度，增强了对网络入侵行为的检测能力。

OpenFire[49]针对网络侦查活动进行欺骗。与传统的防火墙相比，OpenFire 不用阻断不需要的流量，反而会接受所有的流量，将不想要的信息转发给诱饵主机集群。对外来说，所有 OpenFire 网络上的 IP 和端口都是打开的。从攻击者来看，所有的端口和没有使用的 IP 都是开放的，通过这一方案在攻击侦察阶段将攻击者的注意力从真实的服务器吸引到欺骗服务器，作者通过一个 21 天的实验证明了该方案能提高系统的安全性。

针对源自操作系统内部的攻击，Julian 等[50]描述了在操作系统驻留的防御欺骗方法，核心思想是通过在计算机系统中展示虚假 I/O 设备，使感染目标主机的恶意软件无效。这些设备并不是真实存在的，而是真实设备的投影，在恶意软件看来这些设备可以当作攻击其他系统的通道。

通过周期性重新映射网络地址和系统设备之间的绑定可以改变组织网络的拓扑，从而隐藏真实的系统设备。Antonatos 等[21]提出了网络地址随机化（NASR, network address space randomization）的解决方案，使用动态主机配置协议给每个主机重新分配网络地址，以使带有目标列表的蠕虫失效。类似技术还有 MUTE[22]，通过采用随机地址跳变（random address hopping）技术和随机指纹（random finger printing）技术使网络可以随机动态地更改它的配置，以限制攻击者扫描、发现、识别和定位网络目标。Robertson 等[51]提出了用于欺骗和缓解攻击的定制信息网络（CINDAM, customized information networks for deception and attack mitigation）方案，使防御方可以调整网络视图，从而挫败攻击或增加攻击的代价。CINDAM 为网络上的每个主机创建一个独特、虚幻的网络视图，这一视图隐藏存在的资源、模拟不存在的资源。每台主机看到的网络视图都是变化的，从而降低攻击者先前收集到的目标网络信息的价值。大多数网络地址变换方案受有限地址空间的限制，依赖主机的静态域名来映射动态地址，不能抵御利用域名发起的攻击，Wang 等[52]提出基于随机域名和地址跳变（RDAM, random domain name and address mutation）的防御方法，该方法通过一个动态域名方法，增加了攻击者扫描空间，减小了攻击者使用 DNS 查询列表和时间窗口方法命中一台主机的概率。

4.3 数据层欺骗

当攻击者突破了防御设备，入侵到业务网络内部后需要考虑数据层欺骗。数层级欺骗通过部署虚假文件、数据库表项等欺骗攻击者。数据层欺骗是最早采用的网络欺骗方式之一，部署灵活，可以部署在真实的业务系统中，用来检测攻击、暴露其他欺骗资源以及跟踪攻击者。

Stoll 通过在被入侵的计算机系统中放置一些伪造的具有诱惑性名字的文件吸引入侵者访问，为追踪入侵者赢得了时间[29]。为了捕获间谍软件，Border 等[53]设计了 Siren 系统，能够产生蜜标数据序列并将这些数据混杂在正常用户行为之中，对于通过模仿正常用户行为来逃避异常检测系统的攻击者，如果模仿了注入的蜜标序列，则会触发警报。White 提出了一种伪造个人身份信息的方法[54]，并使用伪造的身份信息（PII, personally identifiable information）用于检测内部人员发起的恶意攻击与身份滥用[55]。为了检测 Tor 网络中存在流量监听的出口节点，Chakravarty 等[56]使用含有身份信息的流量访问诱饵服务器，如果攻击者通过截获的身份信息访问预先设置的 IMAP 和 SMTP 服务器，那么就证明本次经过的出口节点存在监听，在 10 个月的时间里测出在匿名通信系统中有 10 个节点存在的流量监听。

文献[5]提出了 Honeywords 方案来保护口令文件，通过在口令文件中增加额外 $N-1$ 个假的身份凭据来加强安全。如果口令文件被偷并被破解，攻击者将会面对 N 个不同的口令，其中，只有一个是正确的。如果攻击者使用任意一个假的口令，将会触发一个告警，系统管理员就会知道口令数据库已经被盗并被破解。

Akiyama 等[57]提出了基于蜜标的欺骗系统 HoneyCirculator 。在沙箱环境中设置服务器地址、用户名、口令等信息作为蜜标，当收集到的恶意软件在沙箱中运行时这些蜜标就会被传送给攻击者，攻击者利用获取的蜜标登录预先设置的蜜罐服务器，并将恶意 URL 插入蜜罐服务器的文件中。通过从被修改的文件提取插入的 URL 就能获取恶意

服务器地址。该方案能够不采用 Web 爬虫而发现恶意网站。

4.4　应用层欺骗

大多数的用户认证技术会对授权尝试返回成功或者失败的回复，这使在线口令猜解攻击能够判断是否猜解成功。针对这一问题，Zhao 等[58]提出了用户可认证（uvauth）计划，欺骗进行在线猜解攻击的攻击者使之认为发现了正确的用户名和密码。uvauth 的目标是将攻击者引导到一个“假”帐号，从而浪费攻击者的资源和监控攻击活动来学习攻击者的目标，如图 7 所示。

WEB、SSH 等服务也经常成为攻击者入侵的目标。GHH(Google hack honeypot)是针对 Web 应用威胁开发的 Web 应用蜜罐，诱骗通过 Google Hacking 技术发起攻击的攻击者[59]。Glastopf 使用软件模拟的方式实现 Web 蜜罐，针对攻击者利用 Web 应用程序漏洞进行攻击的尝试，Glastopf 试图返回攻击者期望的响应，以此欺骗攻击者[60]。Glastopf 可以发现远程文件包含、本地文件包含、SQL 注入等 Web 应用攻击类型。Mueter 等开发了将 Web 应用程序转换为高交互蜜罐的工具（HIHAT, high interaction honeypot analysistoolkit），通过在 Web 应用程序中加入监控模块，从而将 PHP 应用程序转换为蜜罐。为了让攻击者发现蜜罐站点同时正常用户不会发现，Mueter 等[16]提出了通过透明链接部署的方式。Ishikawa 等[61]提出了通过使用 Web 应用程序欺骗代理预防和检测攻击的方法，通过拦截 HTTP 流量，在原有 HTML 中加入新的欺骗参数并对原有参数进行符号化，从而挫败与发现攻击。该方法的好处是不用修改 Web 应用的内容。Thompson 等[62]提出了用于移动目标防御的动态应用程序旋转环境方法（DARE MTD，dynamic application rotation environment for moving target defense）。DARE MTD 使用 2 种免费的 Web 服务器软件 Apache 和 Nginx，在 2 个平台上运行单个应用程序，并以随机时间间隔将入站流量发送到其中一个服务器，通过减少平台暴露于潜在攻击者的时间来减少服务器软件未知漏洞暴露的概率。

Kippo 蜜罐伪装成 SSH 网络服务，对攻击者暴力破解攻击使用的用户名与口令、攻击源 IP 地址、SSH 客户端类型、输入的命令以及攻击工具文件进行捕获与记录[63]。

攻击者可以利用应用程序的响应来判断应用程序上的特定漏洞是否已经修复，针对这一情况，Araujo 等[6]提出了 honey-patches 方案以挫败攻击者利用系统响应判断漏洞修复情况的尝试。当检测到攻击者对漏洞的探测，honey-patch 将攻击者的探测转移到作为诱饵的未打补丁的应用程序，诱饵应用程序将会返回存在漏洞的响应。对诱饵应用程序进行监控就可以收集重要的攻击信息。作者通过使用包括 Apache 在内的 3 个产业级 Web 服务器进行了实现，证明了所提方案的可行性。

网页挂马是入侵中常用的恶意代码投送手段之一。针对这一情况，需要欺骗环境主动访问目标站点以发现威胁。Wang 等[39]开发了自动化 Web 巡逻系统 HoneyMonkey，伪装成正常用户浏览器与网站交互，来自动化的识别和监控恶意网站。Capture-HPC[64]支持在使用 Windows 系统构建的欺骗环境中运行 IE、Firefox 等浏览器，通过系统内核中的状态变化来检测浏览器当前访问的网页中是否包含攻击代码。PhoneyC[65]则采用软件模拟方式模拟已知浏览器与插件漏洞来检测恶意网页，并采

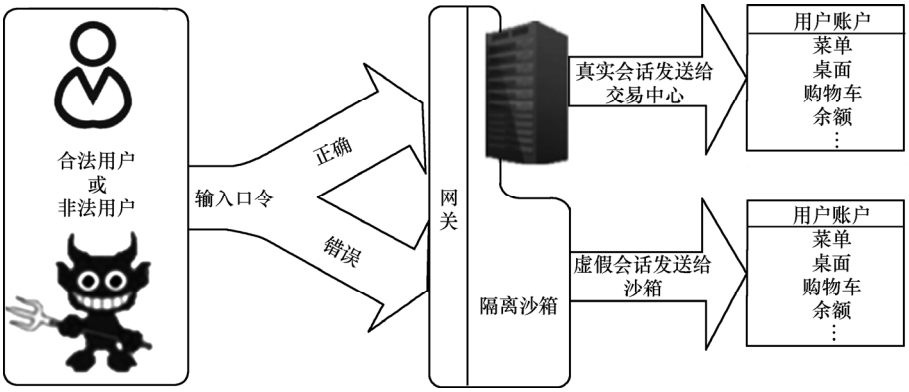


图 7　uvauth 工作流程

用 Javascript 动态分析技术对抗恶意网页脚本混淆机制。恶意网页可以检测客户端的信息来动态重定向 URL，如果客户端蜜罐不符合恶意网页检查的条件，恶意行为就不会被触发，为了应对此类逃避技术，Takata 等[66]提出了一种分析重定向 JS 代码并提取代码中 URL 的方法，并在浏览器模拟器 MineSplider 上实现了该方法。

4.5 基于杀伤链模型的验证

杀伤链（kill chain）来源于军事术语，用来描述攻击行动的过程。洛克希德-马丁公司提出入侵杀伤链来描述计算网络入侵活动[67]。在该模型中入侵被分为 7 个阶段，如表 3 所示。对于不同目的的入侵型攻击来说，差异在于最后的行动阶段。在本节使用入侵杀伤链来分析不同网络欺骗技术的作用阶段，不同网络欺骗技术作用阶段如表 4 所示。

表 3 入侵杀伤链

阶段	描述
侦查	选择与研究目标，寻找目标网络漏洞
武器化	研制网络武器，如病毒和蠕虫
投送	将网络武器投送到目标
漏洞利用	触发网络武器，在目标网络中利用漏洞
安装	网络武器安装可被入侵者使用的接入点
命令与控制	入侵者与目标网络保持访问
执行	入侵者采取行动达到攻击目标，如数据分割、摧毁等

1) 侦查阶段和武器化阶段

攻击者需要识别和确定目标，根据目标环境决定采取的方法，如确定目标操作系统、安全防护软件、应用软件、存在的漏洞等。在此阶段可以通过隐藏操作系统类型、提供虚假设备、提供虚假服务等手段，从而误导攻击者武器的研制以挫败攻击，或将攻击者注意力转移到虚假目标上从而发现攻击。

2) 投送阶段

在此阶段攻击者要将生成的攻击代码发送给受害者以建立初步的立足点。攻击者常用的方法包括钓鱼邮件、水坑攻击、恶意站点等。此时，网络欺骗与边界防御设备相结合，当边界防御设备检测到恶意特征之后则将攻击流量转移到欺骗环境，此种方法依赖于边界防御设备的检测精度。也可以通过改变组织结构外形使得攻击代码被投送到错误的目标。

对于水坑攻击，可以将组织内部人员经常访问的站点形成列表，使用有漏洞的系统“拟人”化模拟用户访问行为以发现存在的威胁，从而保证访问环境的安全。对于钓鱼邮件，可以将邮件中的附件提交到构建的虚拟环境以检查附件的安全性。

3) 漏洞利用阶段和安装阶段

在此阶段可以利用 honey-patches 方案，当检测到针对漏洞的利用企图，honey-patches 透明的将攻击者的探测流量转移到未打补丁的诱饵，诱饵将会返回存在漏洞的响应。同时，可以在系统中留下虚拟机或者蜜罐的特征，使攻击者以为进入了虚拟环境或者蜜罐从而吓阻攻击者。

4) 命令控制与任务执行

执行的任务可以分为 2 种，一种是控制系统以作为跳板进一步渗透，另一种是获取系统上的数据资源。对于以控制系统为主的攻击，任务执行相当于再次发起攻击，即新一轮的侦查，通过在网络中布设诱饵环境可以检测到被控节点。而对于以系统数据为目标的攻击，如果攻击者访问了作为入侵指示器的数据资源同样意味着攻击暴露。

5 网络欺骗对抗技术

在网络欺骗得到安全社区的广泛关注之后，一些黑客与安全研究人员从攻击方角度对网络欺骗

表 4 入侵杀伤链中各个阶段可以采取的网络欺骗技术

欺骗类型	侦查和武器化	投送	漏洞利用和安装	命令控制与武器执行
应用欺骗	Glastopf、HIHAT、Kippo	HoneyMonkey、Capture-HPC、PhoneyC	uvauth、honey-patches	—
数据欺骗	Honeywords、Detecting traffic snooping in Tor using decoys	—	—	PII、honeyfile、Siren
网络结构欺骗	Honeyd、honeynet、混杂蜜罐、OpenFire	Network Address Space Randomization、MUTE（mutable networks）、CINDAM、RDAM		—
设备欺骗	DTK、HoneyBow、Argos、Operating System Obfuscation、FPH	—	fake honeypot	—

识别与绕过等对抗技术展开研究，并提出了一系列对抗现有欺骗技术的机制。因为早期应用比较广的是蜜罐技术，因此这方面的研究主要集中在蜜罐的识别与识别对抗。Chen 等[68]研究显示，有些恶意软件会检测蜜罐并改变自身行为来欺骗蜜罐。从现有的检测机制来看可以分为 3 种：基于特征、基于异常、基于行为。

5.1　基于特征

为了监控攻击者的活动，在使用真实系统作为诱骗环境时往往会安装监控软件，部署方式上常常会采用虚拟化技术。因此通过检测已知蜜罐系统常用监控工具和虚拟化环境可以发现欺骗系统的存在。

在蜜网中常常使用 Sebek 工具监控攻击者的活动，通过对 Sebek 的监控可以发现蜜网环境，如 Dornseif 等[69]针对 Sebek 行为监控组件提出了识别与移的技术方法。针对虚拟机，Holz 等[43]介绍了用户模式 Linux（UML, User Mode Linux）、VMware 虚拟机等可疑环境的识别方法。UML 默认在 Tracing Thread（TT）模式下运行，通过查看进程信息可以发现 TT 模式，同时地址空间、磁盘、文件等都可以用来作为识别 UML 的特征。对于 VMware 可以通过查看系统提供的硬件层与 MAC 地址等进行识别。

5.2　基于异常

欺骗环境与真实业务环境会表现出不同，通过发现这些不同可以检测欺骗环境。

Honeyd 模拟的虚拟网络的延时与真实网络存在差异，文献[70]发现通过在真实网络中远程测量业务网络延时可以发现部署的 Honeyd。低交互蜜罐不会实现全部的协议，往往只是实现有漏洞的部分，Defibaugh-Chavez 等[71]利用这一特征提出了低交互蜜罐检测方法，同时发现虚拟机和低交互蜜罐对于网络应答时间也与真实主机不同。

5.3　基于行为

欺骗环境在部署的过程中会采取风险控制措施，以防止欺骗系统作为攻击的跳板，针对这一行为限制可以作为检测点。

Krawetz 介绍了第一款商业反蜜罐软件 Honeypot Hunter[72]，该软件针对收集垃圾邮件信息的开放代理服务器蜜罐进行识别。通过设置一个虚假的邮件服务器，测试开放代理服务器是否会链接伪装的邮件服务器，如果开发代理返回链接成功而垃圾邮件发送者设置的邮件服务器没有收到开放代理的链接，那么这个开放代理很有可能是一个蜜罐。

Zou 等[73]在僵尸网络的构建与维护过程中引入蜜罐对抗机制。利用安全人员设置的蜜罐不能用于实际攻击的假设提出了对蜜罐敏感的高级僵尸网络构建和维护方法。他们提出的僵尸网络在传播中采用“两阶段侦察”，在攻陷系统后会让被攻陷的系统进一步传播恶意代码，只有被攻陷的系统再次传播恶意代码之后，才会让该系统下载主要代码并加入僵尸网络。文献[73]在此基础上提出了带有伙伴列表的 P2P 僵尸网络构建与维护方法。

5.4　反对抗机制

针对对抗网络欺骗的方法，研究人员也展开了反对抗机制的研究。

对于基于特征的识别方法，可以通过移除用作识别点的特征。Quynh 等[74]在 Xen 虚拟层中实现了对蜜罐系统行为的监控，构建了 Xebek，以代替 Sebek 工具。Jiang 等[75]提出了一种虚拟化部署高交互式蜜罐的外部监控技术，实现了 VMScope 蜜罐行为监控软件。文献[16]则在 Qemu 开源虚拟机中增加断点监控机制，能够更加灵活地提取到各类系统行为记录与运行结果信息。

对于基于异常的识别方法可以通过使得欺骗环境与真实环境更加契合来对抗。Antonatos 等[76]提出了 Honey@home 部署方案。通过在普通用户的系统上安装轻量级的转发模块，监控未用的地址和端口，并将接收到的流量转发到蜜场中，之后将蜜场返回的结果发送给攻击者。因为用户的存在，系统上的活动是动态的，因此，攻击者很难精准地维护一个黑名单。石乐义等[77]结合兵阵的思想，提出动态阵列蜜罐概念，通过多机协同、功能角色的周期或伪随机切换，形成动态变化的阵列陷阱，从而达到迷惑和防范攻击者的目的，使蜜罐系统具有良好的网络对抗性能。

针对基于行为的识别机制，Spampot[78]通过测试邮件识别规则来识别并转发 Spammer 的测试识别邮件，从而避免 Spampot 被 Spammer 加入黑名单。Wang 等[79]设计了动态可扩展双向信道蜜罐（DEH, dynamic extensible honeypot），采用双信道来解决这一问题。如果出口流量包含恶意代码，DEH 就会拦截流量并拷贝恶意代码，然后，DEH 替换恶意代码、

设置双向信道并对恶意攻击者想要攻击的计算机系统设置保护机制，攻击代码会被重定向到蜜罐中或者继续将保护机制扩展到其他系统。

6 结束语

网络欺骗作为一种对抗性技术思路，从诞生开始就得到了学术界和企业界的关注，并涌现出一系列研究成果和工具。本文首先梳理了网络欺骗基本概念并给出了网络欺骗的形式化定义；按照时间顺序将网络欺骗的发展史分为开创阶段、蜜罐阶段和欺骗防御阶段，介绍了各个阶段的特点；根据欺骗的作用点提出了网络欺骗层次化模型对已有技术进行介绍，并结合入侵杀伤链描述不同技术的作用阶段；将已有对抗网络欺骗的技术分为基于特征、基于异常、基于行为 3 种进行介绍，并介绍了防御方针对这些对抗技术采取的应对措施。

现有网络欺骗技术没有形成固定且统一的形态，而是随着攻击技术与网络安全需求的变化而演化，尽管有一些网络欺骗技术的理论研究工作，然而更侧重于对网络欺骗效果的分析，没有成体系的理论基础与通用的标准规范。与其他安全防御措施相比，基于欺骗的防御技术需要防止被入侵者发现，这就要求与业务系统具有高度的一致性，现有的欺骗技术在根据业务系统进行动态调整的能力上还有所欠缺，由安全人员开发的欺骗工具与业务环境契合度尚需完善。欺骗技术的进一步研究工作如下。1)与威胁情报相结合，一方面利用威胁情报提供的信息完善欺骗策略，另一方面欺骗技术捕获到的信息反过来可以助力威胁情报的生成。2)可定制、智能化的网络欺骗技术框架研究与开发，通过机器学习、人工智能等技术根据所部署的业务环境自动生成与业务系统高度一致具有高保密性的欺骗环境。3)研究以 SDN、云平台等技术部署的具有伸缩性的网络欺骗工具。

网络欺骗是一种与攻击者进行博弈的对抗性思维方式，这一技术将随着安全威胁演化而不断地发展与更新，也将得到安全社区的持续研究和关注。

参考文献：

[1] 蔡桂林, 王宝生, 王天佐, 等. 移动目标防御技术研究进展[J]. 计算机研究与发展, 2016, 53(5): 968-987.
CAI G L, WANG B S, WANG T Z, et al. Research and development of moving target defense technology[J]. Journal of Computer Research and Development, 2016, 53(5): 375-378

[2] ZHUANG R, ZHANG S, DELOACH S A, et al. Simulation-based approaches to studying effectiveness of moving-target network defense[C]//National Symposium on Moving Target Research. 2012. 1-12.

[3] JAJODIA S, SUBRAHMANLAN V S, SWARUP V, et al. Cyber deception[M]. Springer, 2016

[4] CANALI D, BALZAROTTI D. Behind the scenes of online attacks: an analysis of exploitation behaviors on the Web[C]//20th Annual Network & Distributed System Security Symposium (NDSS 2013). 2013.

[5] JUELS A, RIVEST R L. Honeywords: making password-cracking detectable[C]//2013 ACM SIGSAC conference on Computer & communications security. 2013: 145-160.

[6] ARAUJO F, HAMLEN K W, BIEDERMANN S, et al. From patches to honey-patches: Lightweight attacker misdirection, deception, and disinformation[C]//The 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014: 942-953.

[7] KAPRAVELOS A, GRIER C, CHACHRA N, et al. Hulk: Eliciting malicious behavior in browser extensions[C]//The 23rd Usenix Security Symposium. 2014.

[8] GUPTA P, SRINIVASAN B, BALASUBRAMANIYAN V, et al. Phoneypot: data-driven understanding of telephony threats[C]//2015 Network and Distributed System Security (NDSS) Symposium. 2015.

[9] URIAS V E, STOUT W M, LIN H W. Gathering threat intelligence through computer network deception[C]// 2016 IEEE Symposium on Technologies for Homeland Security (HST). 2016:1-6.

[10] TAN K L G. Confronting cyberterrorism with cyber deception[D]. Monterey, California: Naval Postgraduate School, 2003.

[11] JONES J H J, LASKEY K B. Using Bayesian attack detection models to drive cyber deception[C]//The Eleventh UAI Conference on Bayesian Modeling Applications Workshop. 2014: 60-69.

[12] 刘宝旭, 许榕生. 主动型安全防护措施-陷阱网络的研究与设计[J]. 计算机工程, 2002, 28(12): 9-11.
LIU B X, XU R S.Study and design of the proactive security protecting measure-honeynet[J]. Computer Engineering, 2002, 28(12): 9-11

[13] 刘宝旭, 曹爱娟, 许榕生. 陷阱网络技术综述[J]. 网络安全技术与应用, 2003, (01): 65-69.
LIU B X, CAO A J,XU R S. Summary of the honeynet technology[J].Net Security Technologies And Application, 2003, (01): 65-69.

[14] 曹爱娟, 刘宝旭, 许榕生. 网络陷阱与诱捕防御技术综述[J]. 计算机工程, 2004, (09): 1-3.
CAO A J, LIU B X, XU R S. Summary of the honeynet and entrapment defense technology[J], Computer Engineering, 2004, (09): 1-3.

[15] 程杰仁, 殷建平, 刘运, 等. 蜜罐及蜜网技术研究进展[J]. 计算机研究与发展, 2008,45 (S1): 375-378.

CHENG J R, YIN J P, LIU Y, et al. Advances in the honeypot and honeynet technologies[J]. Journal of Computer Research and Development, 2008, 45(S1): 375-378

[16] 诸葛建伟, 唐勇, 韩心慧, 等. 蜜罐技术研究与应用进展[J]. 软件学报, 2013,24 (04): 825-842.
ZHUGE J W, TANG Y, HAN X H, et al. Honeypot technology research and application[J]. Journal of Software, 2013, 24(4): 825-842.

[17] WHALEY B. Toward a general theory of deception[J]. The Journal of Strategic Studies, 1982, 5(1): 178-192.

[18] 韩枫. 军事欺骗行为仿真研究[D]. 郑州: 解放军信息工程大学, 2006.
HAN F. Research on emulate of the military deception[D]. Zhengzhou: Information Engineering University, 2006

[19] YUILL J J. Defensive computer-security deception operations: processes, principles and techniques[D]. North Carolina: North Carolina State University, 2006.

[20] ALMESHEKAH M H, SPAFFORD E H. Cyber Security Deception[M]//Cyber Deception. 2016: 25-52.

[21] ANTONATOS S, AKRITIDIS P, MARKATOS E P, et al. Defending against hitlist worms using network address space randomization[J]. Computer Networks, 2007, 51(12): 3471-3490.

[22] AL-SHAER E. Toward network configuration randomization for moving target defense[M]//Moving Target Defense. 2011: 153-159.

[23] ROWE N C, DUONG B T, CUSTY E J. Fake honeypots: a defensive tactic for cyberspace[C]//2006 IEEE Information Assurance Workshop. 2006: 223-230.

[24] MURPHY S, MCDONALD T, MILLS R. An application of deception in cyberspace: operating system obfuscation[C]//5th International Conference on Information Warfare and Security. 2010.

[25] SPITZNER L. The honeynet project: trapping the hackers[J]. IEEE Security & Privacy, 2003, 99(2): 15-23.

[26] 诸葛建伟, 韩心慧, 周勇林, 等. HoneyBow:一个基于高交互式蜜罐技术的恶意代码自动捕获器[J]. 通信学报, 2007, (12): 8-13.
ZHUGE J W, HAN X H, ZHOU Y L, et al. HoneyBow: an automated malware collection tool based on the high-interaction honeypot principle[J]. Journal on Communications, 2007, 28(12): 8-13

[27] YUILL J, ZAPPE M, DENNING D, et al. Honeyfiles: deceptive files for intrusion detection[C]//Information Assurance Workshop. 2004: 116-122.

[28] COHEN F. A note on the role of deception in information protection[J]. Computers & Security, 1998, 17(6): 483-506.

[29] STOLL C P. The cuckoo’s egg: tracing a spy through the maze of computer espionage[M]. Doubleday. 1989.

[30] CHESWICK B. An evening with Berferd in which a cracker is Lured, Endured, and Studied[C]//The Winter 1992 USENIX Conference. 1992: 163-174.

[31] KIM G H, SPAFFORD E H,Experiences with tripwire: using integrity checkers for intrusion detection[R]. Purdue University, Department of Computer Sciences, 1994.

[32] COHEN F. A mathematical structure of simple defensive network deceptions[J]. Computers & Security, 2000, 19(6): 520-528.

[33] SPITZNER L. Honeypots: tracking hackers[M]. Addison-Wesley Reading, 2003.

[34] DAGON D, QIN X, GU G, et al. Honeystat: local worm detection using honeypots[C]//International Workshop on Recent Advances in Intrusion Detection. 2004: 39-58.

[35] CRANDALL J R, WU S F, CHONG F T. Experiences using minos as a tool for capturing and analyzing novel worms for unknown vulnerabilities[C]//International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. 2005: 32-50.

[36] KREIBICH C, CROWCROFT J. Honeycomb: creating intrusion detection signatures using honeypots[J]. ACM SIGCOMM computer communication review, 2004, 34(1): 51-56.

[37] SCHRYEN G. An e-mail honeypot addressing spammers' behavior in collecting and applying addresses[C]//6th Annual IEEE Systems, Man and Cypernetics Information Assurance Workshop. 2005: 37-41.

[38] SCHRYEN G. The impact that placing email addresses on the Internet has on the receipt of spam: an empirical analysis[J]. Computers & Security, 2007, 26(5): 361-372.

[39] WANG Y M, BECK D, JIANG X, et al. Automated Web patrol with strider honeymonkeys[C]//The 2006 Network and Distributed System Security Symposium. 2006: 35-49.

[40] BAECHER P, KOETTER M, HOLZ T, et al. The nepenthes platform: An efficient approach to collect malware[C]//9th International Symposium on Recent Advances in Intrusion Detection. Hamburg, GERMANY, 2006. 165-184.

[41] PORTOKALIDIS G, SLOWINSKA A, BOS H. Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation[C]//The 2006 EuroSys Conference. 2006: 15-27.

[42] NEWSOME J, SONG D. Dynamic taint analysis for automatic detection, analysis, and signaturegeneration of exploits on commodity software[C]//The 12th Annual Network and Distributed System Security Symposium. 2005.

[43] HOLZ T, RAYNAL F. Detecting honeypots and other suspicious environments[C]//6th Annual IEEE Systems, Man and Cypernetics Information Assurance Workshop. 2005: 29-36.

[44] ROWE N C, CUSTY E J, DUONG B T. Defending cyberspace with fake honeypots[J]. Journal of Computers, 2007, 2(2): 25-36.

[45] ZHAO Z, LIU F, GONG D. An SDN-based fingerprint hopping method to prevent fingerprinting attacks[J]. Security and Communication Networks, 2017.

[46] DISSO J P, JONES K, BAILEY S. A plausible solution to scada security honeypot systems[C]//2013 Eighth International Conference on

Broadband and Wireless Computing, Communication and Applications (BWCCA). 2013: 443-448.

[47] PROVOS N. Honeyd-a virtual honeypot daemon[C]//10th DFN-CERT Workshop. 2003.

[48] ARTAIL H, SAFA H, SRAJ M, et al. A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks[J]. Computers & Security, 2006, 25(4): 274-288.

[49] BORDERS K, FALK L, PRAKASH A. OpenFire: using deception to reduce network attacks[C]//3rd International Conference o Security and Privacy in Communication Networks and Workshops. 2007: 224-233.

[50] RRUSHI J L. NIC displays to thwart malware attacks mounted from within the OS[C]//Computers & Security. 2016: 6159-6171.

[51] ROBERTSON S, ALEXANDER S, MICALLEF J, et al. CINDAM: customized information networks for deception and attack mitigation[C]//IEEE 9th International Conference on Self-Adaptive and Self-Organizing Systems Workshops, Massachusetts Inst Technol. 2015: 114-119.

[52] WANG K, CHEN X, ZHU Y. Random domain name and address mutation (RDAM) for thwarting reconnaissance attacks[J]. Plos One, 2017, 12(5): e0177111.

[53] BORDERS K, ZHAO X, PRAKASH A. Siren: catching evasive malware[C]//2006 IEEE Symposium on Security and Privacy (S&P'06). 2006.

[54] WHITE J. Creating personally identifiable honeytokens[M]//Innovations and Advances in Computer Sciences and Engineering. Springer. 2010: 227-232.

[55] WHITE J, PANDA B. Implementing PII honeytokens to mitigate against the threat of malicous insiders[C]//2009 IEEE International Conference on Intelligence and Security Informatics. 2009: 233.

[56] CHAKRAVARTY S, PORTOKALIDIS G, POLYCHRONAKIS M, et al. Detecting traffic snooping in Tor using decoys[C]//International Workshop on Recent Advances in Intrusion Detection. 2011: 222-241.

[57] AKIYAMA M, YAGI T, HARIU T, et al. HoneyCirculator: distributing credential honeytoken for introspection of web-based attack cycle[J]. International Journal of Information Security, 2017, 1-17.

[58] ZHAO L, MANNAN M. Explicit authentication response considered harmful[C]//The 2013 New security paradigms workshop (NSPW'13). 2013: 77-86.

[59] JOHN J P, YU F, XIE Y, et al. Heat-seeking honeypots: design and experience[C]//The 20th International Conference on World Wide Web. 2011: 207-216.

[60] MPHAGO B, BAGWASI O, PHOFUETSILE B, et al. Deception in dynamic Web application honeypots: case of glastopf[C]//The International Conference on Security and Management (SAM). 2015: 104.

[61] ISHIKAWA T, SAKURAI K. Parameter manipulation attack prevention and detection by using web application deception proxy[C]//The 11th International Conference on Ubiquitous Information Management and Communication. 2017: 74.

[62] THOMPSON M, MENDOLLA M, MUGGLER M, et al. Dynamic application rotation environment for moving target defense[C]//2016 Resilience Week. 2016.

[63] VALLI C, RABADIA P, WOODWARD A. Patterns and patter-an investigation into SSH activity using kippo honeypots[C]//The 11th Australian Digital Forensics Conference. 2013: 141-149.

[64] HES R, KOMISARCZUK P, STEENSON R, et al. The capture-HPC client architecture[R]. Technical report, Victoria University of Wellington, 2009.

[65] NAZARIO J. PhoneyC: a virtual client honeypot[C]//The 2nd USENIX Conference on Large-scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More. 2009: 1-8.

[66] TAKATA Y, AKIYAMA M, YAGI T, et al. MineSpider: extracting hidden URLs behind evasive drive-by download attacks[J]. Ieice Transactions on Information & Systems, 2016, E99.D(4): 860-872.

[67] HUTCHINS E M, CLOPPERT M J, AMIN R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[J]. Leading Issues in Information Warfare & Security Research, 2011, 180.

[68] CHEN X, ANDERSEN J, MAO Z M, et al. Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware[C]//2008 IEEE International Conference on Dependable Systems & Networks With FTCS & DCC. 2008: 177-186.

[69] DORNSEIF M, HOLZ T, KLEIN C N. Nosebreak-attacking honeynets[C]//5th Annual IEEE Information Assurance Workshop. 2004: 123-129.

[70] FU X, YU W, CHENG D, et al. On recognizing virtual honeypots and countermeasures[C]//2nd IEEE International Symposium on Depenable, Autonomic and Secure Computing. 2006: 211-218.

[71] DEFIBAUGH-CHAVEZ P, VEERAGHATTAM R, KANNAPPA M, et al. Network based detection of virtual environments and low interaction honeypots[C]//7th Annual IEEE Information Assurance Workshop. 2006: 283-289.

[72] KRAWETZ N. Anti-honeypot technology[J]. IEEE Security & Privacy, 2004, 2(1): 76-79.

[73] ZOU C C, CUNNINGHAM R. Honeypot-aware advanced botnet construction and maintenance[C]//International Conference on Dependable Systems and Networks (DSN'06). 2006: 199-208.

[74] QUYNH N A, TAKEFUJI Y. Towards an invisible honeypot monitoring system[C]//11th Australasian Conference on Information Security and Privacy. Melbourne, AUSTRALIA, 2006: 111-122.

[75] JIANG X, WANG X. “Out-of-the-box” monitoring of VM-based

high-interaction honeypots[C]//International Workshop on Recent Advances in Intrusion Detection. 2007: 198-218.

[76] ANTONATOS S, ANAGNOSTAKIS K, MARKATOS E. Honey@home: a new approach to large-scale threat monitoring[C]//5th ACM Workshop on Recurring Malcode. 2007: 38-45.

[77] 石乐义, 李婕, 刘昕, 等. 基于动态阵列蜜罐的协同网络防御策略研究[J]. 通信学报, 2012, (11): 159-164.
SHI L Y, LI J, LIU X, et al. Research on dynamic array honeypot for collaborative network defense strategy[J]. Journal on Communications, 2012, 33(11): 159-164.

[78] 郭军权, 诸葛建伟, 孙东红, 等. Spampot:基于分布式蜜罐的垃圾邮件捕获系统[J]. 计算机研究与发展, 2014, 51(5): 1071-1080.
GUO J Q, ZHUGE J W, SUN D H, et al. Spampot: a spam CAPTURE system based on distributed honeypot[J]. Journal of Computer Research & Development, 2014, 51(5):1071-1080

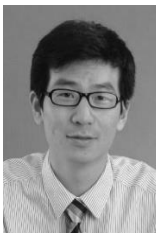
[79] WANG C Y, JHAO Y L, WANG C S, et al. The bilateral communication-based dynamic extensible honeypot[C]//49th Annual International Carnahan Conference on Security Technology (ICCST). 2015: 263-268.

作者简介：

贾召鹏（1988-），男，河北邢台人，北京邮电大学博士生，主要研究方向为网络安全、网络欺骗。

方滨兴（1960-），男，江西万年人，中国工程院院士，广州大学教授，主要研究方向为计算机体系结构、计算机网络与信息安全。

刘潮歌（1986-），男，吉林长春人，中国科学院信息工程研究所助理研究员、博士生，主要研究方向为 Web 安全、网络欺骗、追踪溯源。



刘奇旭（1984-），男，江苏徐州人，博士，中国科学院信息工程研究所副研究员，中国科学院大学副教授，主要研究方向为网络攻防技术、网络安全评测。

林建宝（1992-），男，山东威海人，北京邮电大学硕士生，主要研究方向为网络安全、网络欺骗。