云计算环境下的隐蔽信道分析

丁丽萍

中国科学院软件研究所基础软件国家工程研究中心

提纲

- 隐蔽信道概述
  - 概念分类
  - 研究现状
- 云计算环境下的安全威胁与隐蔽信道
  - 云计算的安全威胁
  - 云计算安全威胁分析
- 我们的工作
  - 基于XCP的隐蔽信道
  - 基于XCP的隐蔽信道的实例
  - 基于XCP的隐蔽信道的分类
  - 基于XCP的隐蔽信道分析技术

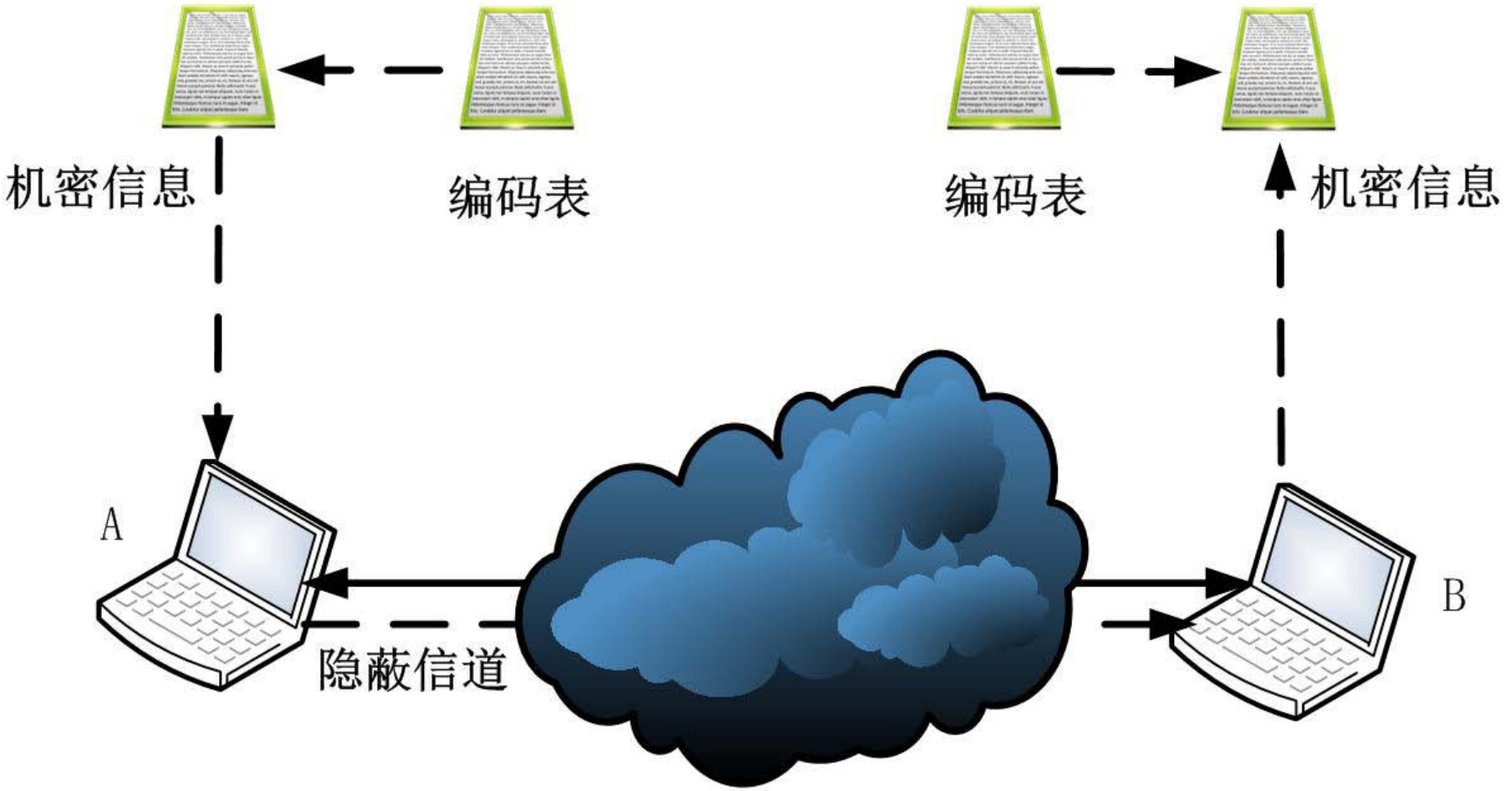
隐蔽信道的概念

- 隐蔽信道定义
  - 隐蔽信道是指恶意进程通过合谋信息系统共享资源而实现的一种信息泄漏方式。
- 隐蔽信道分析
  - 隐蔽信道分析是国内外安全标准对脆弱性分析的强制性要求。
  - 具体分析工作包括信道的识别、度量和处置。
  - 隐蔽通道分析是信息安全研究领域的一个重要难题，其原因在于：以强制访问控制研究为基础；海量代码分析复杂；技术壁垒导致参考资料非常少。

隐蔽信道分析

- 信道识别是对系统的静态分析，强调对设计和代码进行分析以发现所有潜在的隐蔽信道。
- 信道度量是对信道传输能力和威胁程度的评价。
- 信道处置措施包括信道消除、限制和审计:
  - 隐蔽信道消除措施包括修改系统、排除产生隐蔽信道的源头、破坏信道的存在条件。
  - 限制措施要求将信道危害降低到系统能够容忍的范围内。
  - 隐蔽信道审计则强调对潜在隐蔽信道的相关操作进行监测和记录，通过分析记录，检测出入侵者对信道的实际使用操作。

隐蔽信道关键技术



隐蔽信道关键技术

- 隐蔽信道本质上是信息传输通道，传输机制的研究重点集中在对传输介质的研究。根据共享资源属性的不同，传输介质分为存储类型和时间类型，由此衍生出存储隐蔽信道和时间隐蔽信道的分类。
  - 在操作系统、数据库、网络系统中都存在存储隐蔽信道和时间隐蔽信道。
  - 在操作系统、数据库或者网络中发现一种共享资源作为隐蔽信道的传输介质，是隐蔽信道传输机制的核心，而好的传输介质的选择，能够提高信道的容量和隐匿性。

隐蔽信道关键技术

- 提高隐蔽信道的传输准确率和隐匿性的另一种方式是改进信道的编解码机制。
  - 利用字母的频率特征，编码期望长度较大。如果在编码过程中考虑频率特征，则会降低期望长度、减少隐蔽信道中传输的数据量。
  - 多元编码机制虽然增加了收发双方的编解码工作量，但整体上压缩了传输数据量、提高了信道容量。同时多元编码分散了共享资源属性特征出现频率，提高了隐匿性。如果配合纠错协议，能够大幅降低编码错误率。

操作系统隐蔽信道

- 操作系统隐蔽信道研究重点在于防患于未然，侧重于信道标识、场景构建和容量度量。
  - Kemmerer认为隐蔽信道是使用不是正常数据客体的项从一个主体向另一个主体传递信息的信道，并由该定义设计出共享资源矩阵法。该方法构建共享资源矩阵工作量巨大，容易产生状态爆炸。
  - Tsai等人认为隐蔽信道是违反强制安全策略模型的两个主体间的非法通信。提出语义信息流方法，分析编程语言的语义、内核代码中的数据结构，发现其中变量的可修改性/可见性；然后利用信息流分析方法来判断内核变量的间接可见性，以此发现潜在的隐蔽信道。该方法工作量大、缺少自动化工具的缺点。

操作系统隐蔽信道

- Denning对信息流模型进行了形式化描述，为从每个语句中抽象出信息流语义包含“明流”和“暗流”，将信息流策略应用于系统的顶层规范或者代码上，生成信息流公式，最后利用定理证明器证明。
- 卿斯汉延续了语义信息流的思想，设计了一种代码层次的标识方法回溯搜索法，该方法引入“剪枝规则”，在标识过程中立即删除不能构成隐蔽信道的共享变量，显著地减少了分析的工作量。
- Goguen认为，在安全系统中一个用户不能意识到任何不由它所支配的用户的任何操作，称为无干扰模型。如果不存在隐蔽信道，则任何一个用户都应该与其支配的任何用户之间满足无干扰关系。

数据库系统隐蔽信道

- 在数据库系统中存在大量的共享资源，导致隐蔽信道的存在。数据库系统隐蔽信道研究主要集中在信道检测、威胁度量和限制技术中。
- 数据库存储资源引入的信道。该信道利用数据库中的共享资源，如数据、数据字典等。发送者修改数据/数据字典，接收者则通过完整性约束等方式间接感知数据/数据字典的修改，以此来传输机密信息。
- 数据库管理资源引入的信道。数据库系统中的另一类共享资源包括系统变量、游标、临时数据区等。通过耗尽有限的共享资源，收发双方传输机密信息。
- 事务并发控制引起的隐蔽信道。入侵者可以利用不同安全级事务间的并发冲突构造隐蔽信道，称作数据冲突隐蔽信道。

网络系统隐蔽信道

- 网络隐蔽信道将信息泄漏威胁从系统内部转移到系统之间
  - 网络存储隐蔽信道将信息附加在不常用的数据段中，包括未用的IP头字段(ToS字段、DF和URG位)、IP头的扩展和填充段、IP标识和碎片偏移等。
  - 网络时间隐蔽信道将隐蔽信息编码成数据包的发送/到达时刻，时间间隔等序列，更加难以检测和处置。
  - 2004年美国Purdue大学的Cabuk提出一种IP时间隐蔽信道，称作IPCTC。
  - 2009年Purdue大学的Sellke[73]中提出了一种基于编码表的网络时间隐蔽信道，称为$L-bits-to-n-Packets$信道。
  - 现有的网络时间隐蔽信道研究成果可以发现，改进信道的编解码过程能够提高信道容量。

提纲

- 隐蔽信道概述
  - 概念分类
  - 研究现状
- 云计算环境下的安全威胁与隐蔽信道
  - 云计算的安全威胁
  - 云计算安全威胁分析
- 我们的工作
  - 基于XCP的隐蔽信道
  - 基于XCP的隐蔽信道的实例
  - 基于XCP的隐蔽信道的分类
  - 基于XCP的隐蔽信道分析技术

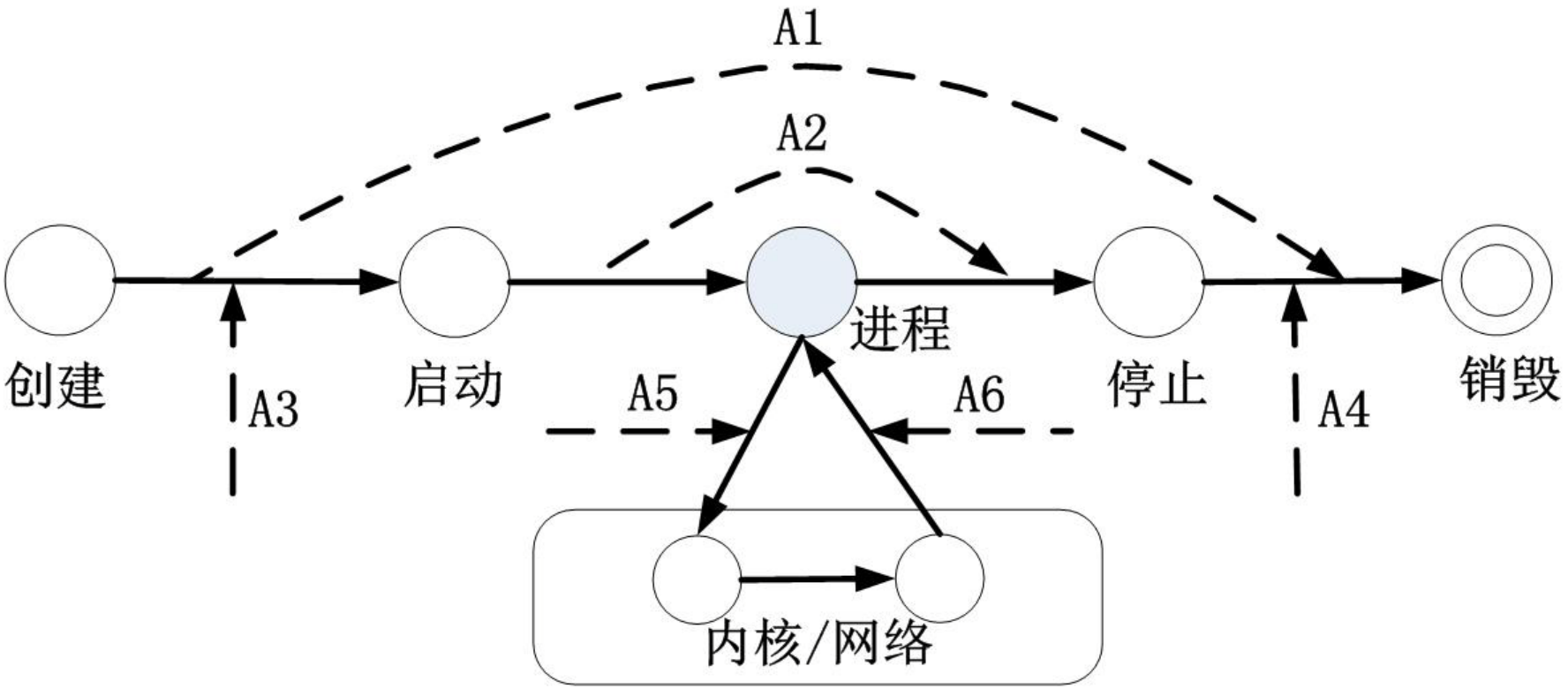
云计算安全威胁

云计算将基础设施、平台及应用部署到云端，无论是从观念上还是技术上都给信息安全带来极大的挑战。

- 入侵者：云计算平台为其提供了一个廉价、高效、稳定的入侵平台。
- 用户：担心将应用程序与服务部署在不可控的环境中的安全性。
- 服务商：由于隐私保护和商业规则，云服务商无法记录和监控客户执行的操作，导致信息泄漏等攻击方式难以记录和发现。

云计算安全威胁分析

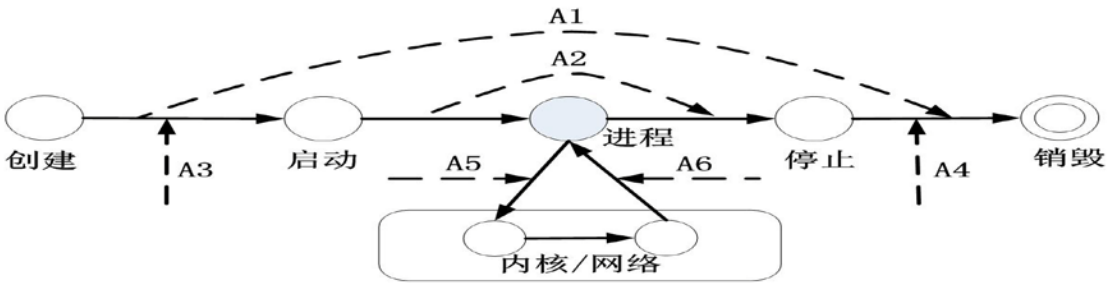
虚拟化技术是云计算平台的核心。虚拟化技术提供了大量的共享资源，成为隐蔽信道发生的源泉。我们以一个虚拟机的生命周期为例来分析云计算面临的威胁。



云计算安全威胁分析

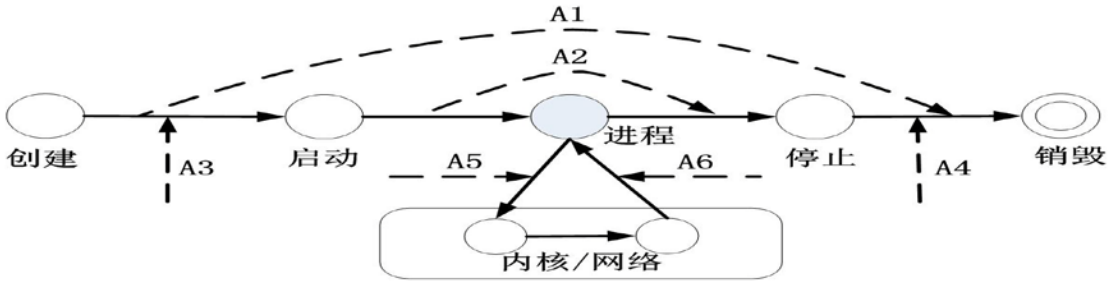
虚拟机运行阶段(A1,A2)

- A1表示虚拟机之间基于共享资源的隐蔽信道
  - 例如，基于CPU负载和Cache缓存的隐蔽信道。在云计算平台中，虽然VMM为每个虚拟机分配了虚拟CPU，但是最终的任务仍然要顺序地在物理CPU上执行，通过观察物理CPU的负载状况，能够推测同一物理平台上其他虚拟机内的机密信息；基于Cache缓存的隐蔽信道类似于CPU负载信道，通过使用Cache的延迟时间，泄漏虚拟机的机密信息。
- A2表示虚拟机内部的隐蔽信道
  - 例如，针对Linux操作系统的事件标识型隐蔽信道，该信道的收发双方通过改变和观察特定事件的状态，合谋传递机密信息。
- A1和A2分别表示了虚拟机外部和内部的两种信息泄漏方式，这两种方式在虚拟机和操作系统层都是不可避免的，即使部署了强制访问控制策略，仍然无法彻底清除隐蔽信道。



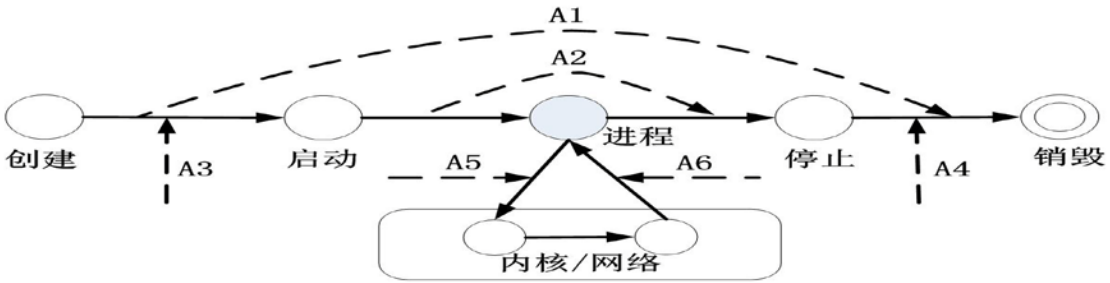
云计算安全威胁分析

- 启动与停止阶段(A3,A4)
  - 云计算的易用性允许恶意用户在短时间内启动和部署大量的计算机节点，用于恶意攻击，例如用于DDoS、Botnet或者对于机密信息的暴力破解。
- A3表示篡改启动镜像类型的攻击
  - 恶意用户篡改替换VM启动的镜像文件，导致客户在云服务的启动阶段就已经被植入恶意程序，成为入侵者的攻击对象。
- A4表示篡改持久化数据的虚拟机攻击方式
  - 当虚拟机将客户数据写入到持久化设备中时，将客户信息泄露给攻击者，或者造成客户数据的故意丢失。
- A3和A4两种攻击类型都是针对云平台的新的攻击方式，可以采用完整性策略对系统进行安全防范。



云计算安全威胁分析

- 应用程序运行阶段(A5,A6)
  - 对终端用户而言，云计算的服务最终由应用程序提供，恶意软件和风险程序是其重要威胁。
- A5表示木马或者病毒攻击方式
  - 当执行内核的系统调用时，木马程序劫持调用并执行恶意操作破坏系统。
- A6表示返回值篡改攻击
  - 木马劫持程序并返回错误的结果从而破坏系统安全，例如缓冲区溢出攻击等。
- 在网络环境中，A5和A6表示中间人攻击方式和其他的网络攻击方式，劫持网络会话执行恶意操作。在云计算环境下，基于Web2.0的攻击方式和基于浏览器的信息泄漏方式，都对系统造成重要威胁。应用层攻击处在虚拟机内部，并不是云计算的新型产物，涵盖了传统的攻击方式。



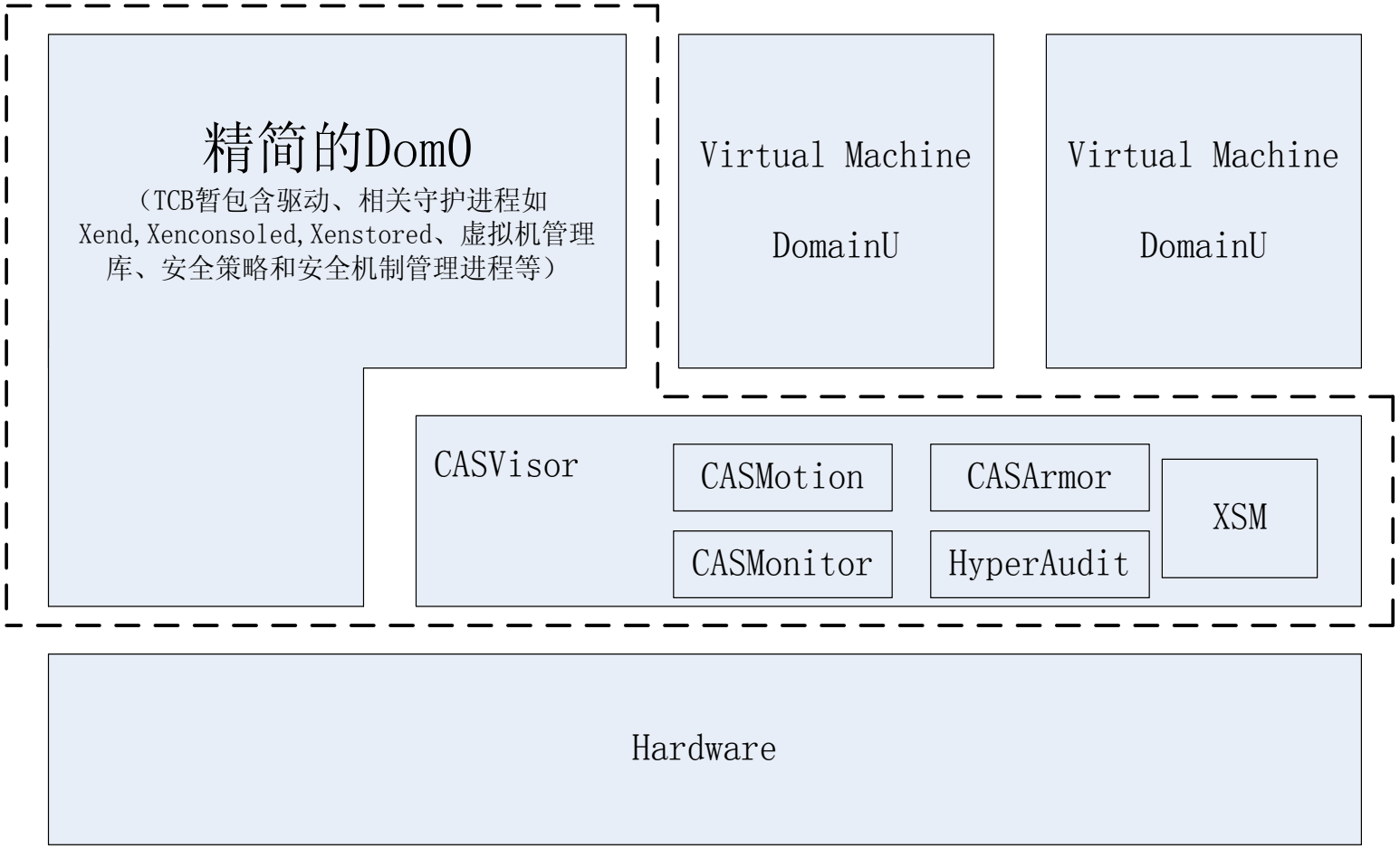
云计算安全威胁总结

- 这三种类型的安全威胁覆盖了云服务的完整的生命周期。按照由低向高的层次，可视为针对**VMM**、**VM**和应用程序的攻击。
- 前两种攻击方式利用了云计算平台动态易用、资源共享的特点，是安全研究领域的新问题。基于应用程序的攻击虽然是传统的研究领域，但是随着计算机技术的飞速发展，攻击方式和攻击手段不断创新，消除和防范技术愈发复杂。
- 通过安全策略，配置私有云、公有云、混合云可以创建相对安全的、灵活实用的云平台。然而，即使部署了安全策略，只要存在资源共享，就不可避免地产生隐蔽信道导致信息泄漏。因此隐蔽信道问题是云计算安全研究的关键问题。

提纲

- 隐蔽信道概述
  - 概念分类
  - 研究现状
- 云计算环境下的安全威胁与隐蔽信道
  - 云计算的安全威胁
  - 云计算安全威胁分析
- 我们的工作
  - 基于XCP的隐蔽信道
  - 基于XCP的隐蔽信道的实例
  - 基于XCP的隐蔽信道的分类
  - 基于XCP的隐蔽信道分析技术

Xen的体系结构


精简的Dom0
（TCB暂包含驱动、相关守护进程如Xend, Xenconsoled, Xenstored、虚拟机管理库、安全策略和安全机制管理进程等）
Virtual Machine
DomainU
Virtual Machine
DomainU
CASVisor
CASMotion
CASArmor
XSM
CASMonitor
HyperAudit
Hardware

基于XCP的隐蔽信道分析

- 云计算平台以虚拟机为基础设施，提供了高度的隔离性，支持不同操作系统和应用程序同时运行。然而由于存在大量的共享资源，隐蔽信道问题是不可避免的。
  - 为了完成虚拟机域间的通信与协作，**Xen**提供了两类共享资源，即超级调用和事件通道。事件通道是**Xen**用于**Domain**和**VMM**之间、**Domain**和**Domain**之间的异步事件通知机制。
  - 事件通道机制与超级调用机制一起完成**VMM**和**Domain**之间的控制和交互：使用超级调用产生从**Domain**到**VMM**的同步调用；使用异步事件机制完成从**VMM**到**Domain**的通知传递。

基于XCP的隐蔽信道实例

- 基于共享内存的隐蔽信道
  - 为了实现虚拟机Domain之间的共享内存，Xen提供了基于超级调用和事件通道的授权表机制。
  - 每个Domain都拥有自己的授权表，DomA创建一个环形数据结构并赋给其他虚拟域如DomB访问权限，以此构成共享内存。
  - 当DomA向共享内存中填充数据后，会通过异步通知机制通知DomB来访问数据，DomB申请中断获取共享内存中的数据。
  - 在传输过程中，如果DomA控制共享内存填充时间，DomB观察获取数据的时间，能够根据时间的不确定性特征，构成基于共享内存的时间隐蔽信道(Sharing Memory Covert Timing Channel)。

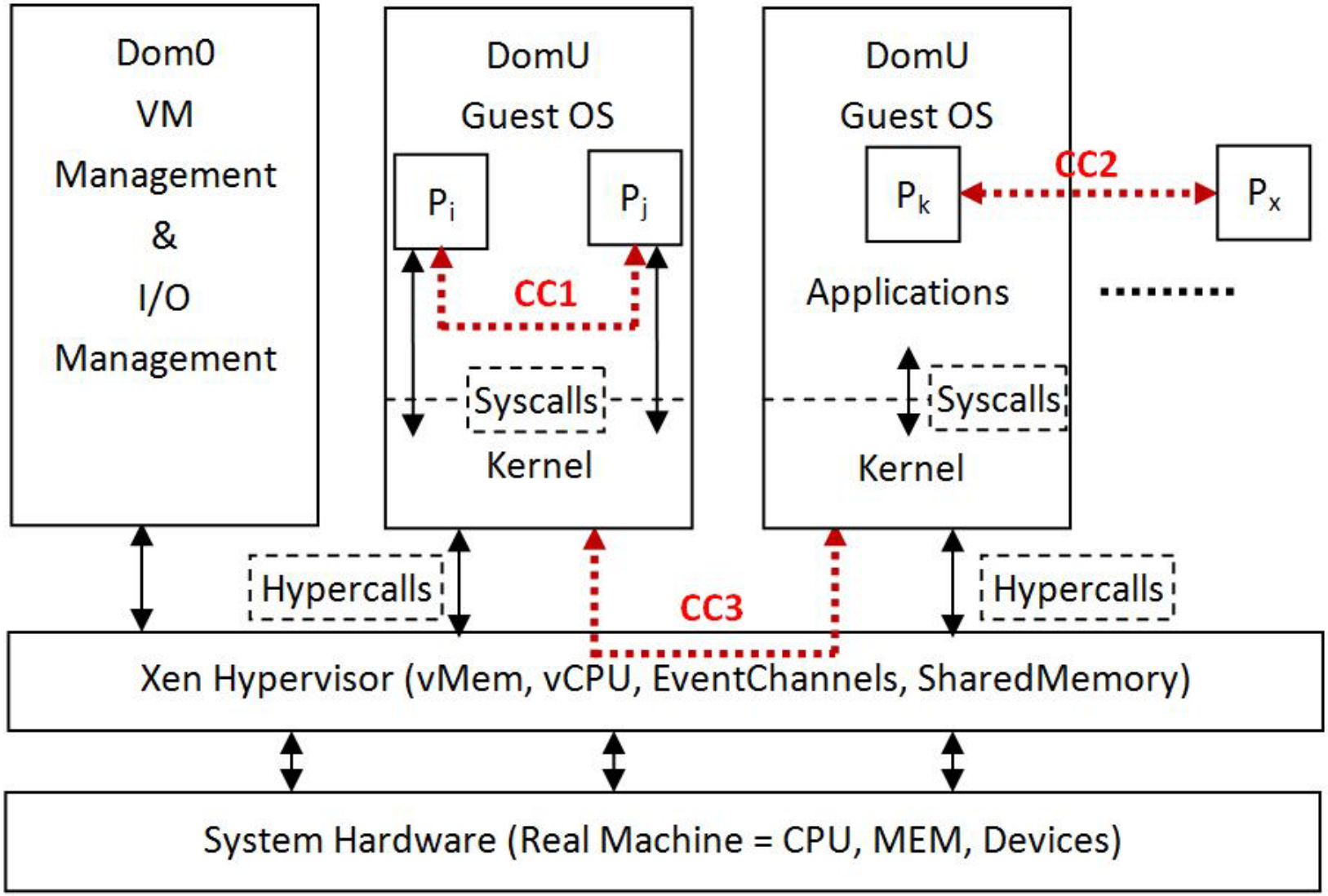
基于XCP的隐蔽信道实例

- 基于Cache/CPU负载的隐蔽信道
  - 2009年，Thomas等研究人员指出处在不同虚拟机之间的进程如果存在硬件资源共享就可能产生隐蔽信道。
  - 基于物理Cache缓存的隐蔽信道：在该信道中，信道发送端用不执行操作和执行大量内存访问操作来表示信息0和1；接收端访问内存并观察访问延迟时间。如果延迟相对较大，说明接收端的内存访问需要先清除接收端的Cache缓存，这意味着发送端执行了大量内存访问且正在传输信息1；如果延迟相对较低，则表示发送端保持沉默，发送信息0。
  - 基于CPU负载的隐蔽信道：类似于基于Cache缓存的隐蔽信道，CPU负载信道也是观测进程执行操作的响应时间，用不同的时间表示不同的信息。

基于XCP的隐蔽信道分类

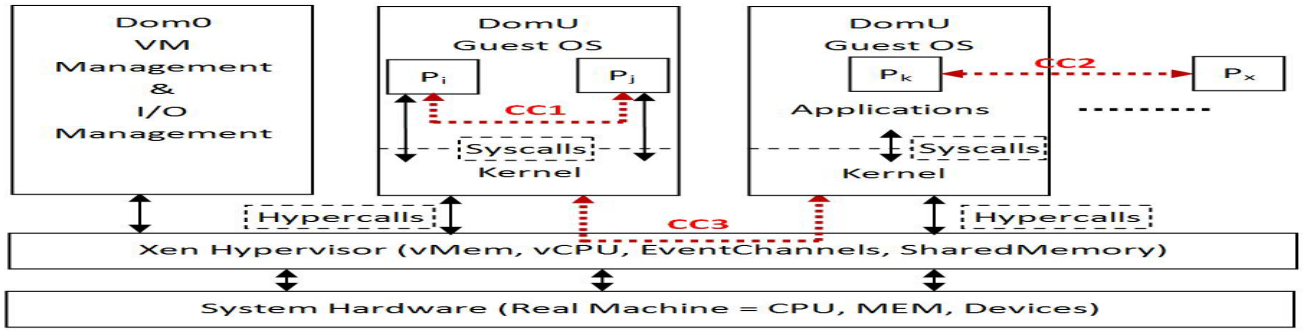
- 隐蔽信道为<V, PA_h, PV_l, P>，变量V可以表示系统中共享资源的不同属性。
  - 当V表示存储属性时，隐蔽信道为存储隐蔽信道。当V表示CPU时间或者其他与时间相关联的属性时，隐蔽信道为时间隐蔽信道。
  - 隐蔽信道本质上是信息的通信信道，因此可以分为噪音信道和无噪信道。
- 现有的研究对隐蔽信道的分类基本上都是出于对工程实践的考虑。这些分类方式并没有体现出隐蔽信道在云计算环境中的特点，所以需要新的分类方式以更准确地刻画隐蔽信道的外延和内涵。

基于XCP的隐蔽信道分类



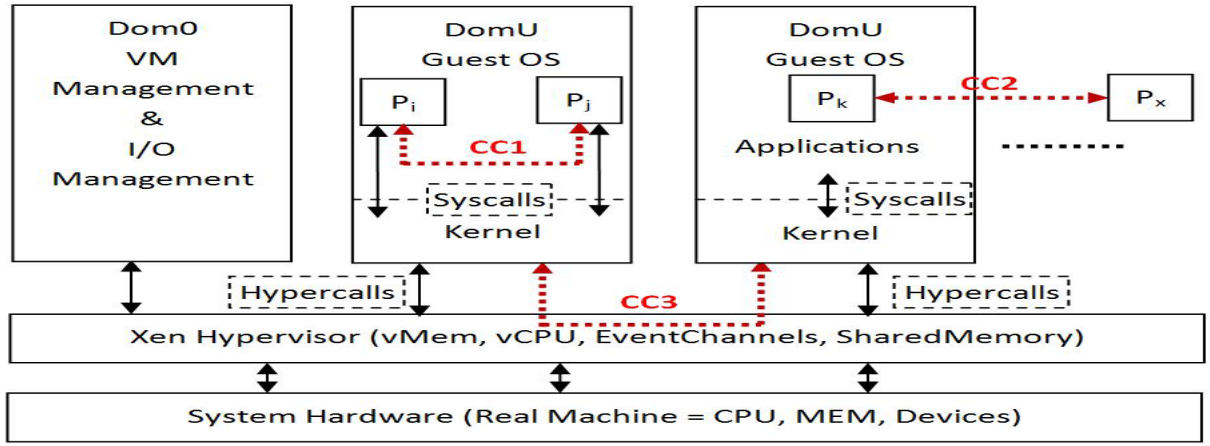
域内隐蔽信道

- 域内隐蔽信道CC1，进程级泄漏方式
  - 恶意进程P_i和P_j处在同一虚拟域(DomU)中，由于虚拟机提供的强隔离性机制，隐蔽信道影响的范围局限在该虚拟域内。DomU中运行独立的操作系统，P_i和P_j是处于不同安全级的操作进程，隐蔽信息从高等级进程泄漏到低等级进程，从而实现隐蔽信道通信。
  - CC1类型的隐蔽信道是操作系统中的进程级机密信息泄漏方式，对其的标识、度量、消除、限制、审计和检测等方法可以参考操作系统隐蔽信道的分析方法。



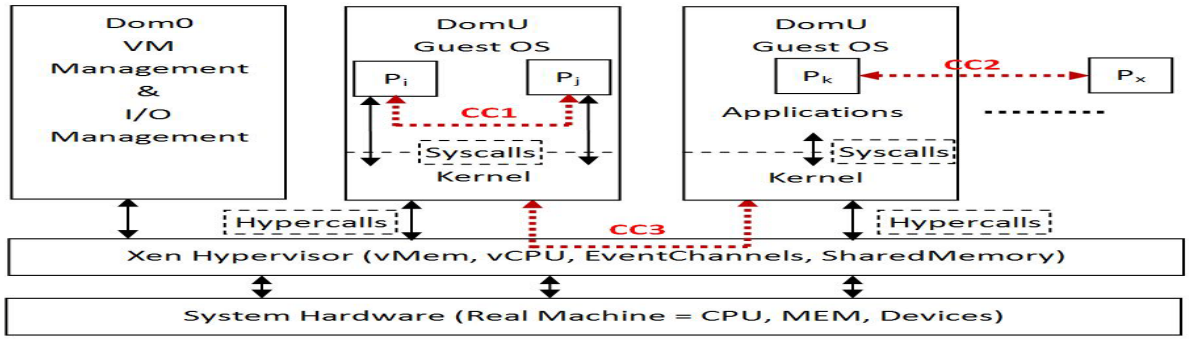
跨平台隐蔽信道

- 跨平台隐蔽信道CC2，网络级隐蔽信道
  - 恶意进程P_k在虚拟机平台DomU中，P_x是其他硬件平台上虚拟机或者独立操作系统中的进程。进程P_k和P_x只能通过网络连接通信，因此CC2信道可抽象为网络隐蔽信道。
  - 对CC2类型信道的研究可以参考传统的网络隐蔽信道研究方法。



域间隐蔽信道

- 域间隐蔽信道CC3，系统级泄漏方式
  - 收发双方恶意进程分处同一硬件平台上不同的虚拟域(DomU)中，机密信息经过操作系统级的传输，泄漏给恶意用户。
  - CC3类型的隐蔽信道是云计算环境中特有的隐蔽信道类型，是由硬件资源共享导致的信道，如基于共享内存、Cache和CPU负载的信道。CC3信道对于云计算客户的数据安全至关重要，如果具有业务竞争关系的客户处在同一物理平台上，CC3类型的信息泄漏将带来沉重的经济代价。



分析过程

- 云计算环境下的隐蔽信道分析需要重点对CC3类型的信道做分析，CC1和CC2类型的信道可以直接采用以前的分析结果。对CC3类型信道分析的过程如下：
  - 安装配置LLVM编译系统;
  - 修改系统源代码的Makefile文件，使之调用LLVM进行编译;
  - 使用编写的中间代码分析工具和信息流图构建工具，查找潜在隐蔽信道;
  - 在系统中部署检查到的潜在隐蔽信道，验证其是否能在真实场景下实现;
  - 通过实验计算其容量;
  - 设计相应的隐蔽信道处置措施。

采用的分析方法

- 基于源代码的有向信息流图标识方法
  - 按照高内聚、低耦合的规则将规模庞大的系统划分为相对独立的多个子系统;
  - 采用*LLVM*编译技术，将分析对象编译成等价的更具结构性的中间代码;
  - 针对中间代码设计查找算法，分析模块中共享资源和操作进程;
  - 结合信息流分析技术，为查找到的共享资源和操作进程创建有向信息流图;
  - 设计有向图搜索和剪枝算法，查找满足隐蔽信道定义的共享资源，即为潜在的隐蔽信道。

专利之一：一种隐蔽信道标识方法

本发明公开了一种基于有向信息流图的隐蔽信道标识方法，以系统源代码为分析对象，提出了一种标识隐蔽信道的新方法。该方法首先形式化描述了安全信息系统中的隐蔽信道<V, PA_h, PV_l, P>，该表述指明隐蔽信道不可或缺的基本要素；然后将待分析的完整系统划分成相对独立的子系统；在每个子系统中以共享变量为基本单元搜索相关的函数调用分支，进而根据信息流关系构建有向信息流图；并根据隐蔽信道的形式化描述对每个信息流图进行剪枝，消除代码中的无效流分支和变量别名；最后得到的所有的信息流图中的变量节点和函数调用分支即为潜在的隐蔽信道组成因素。本发明适用于高安全等级的操作系统，数据库，网络等信息系统的源代码，具有广泛的应用范围、较高的执行效率、较低的误报率和漏报率，能标识系统中的潜在隐蔽信道，满足安全标准对隐蔽信道分析的要求。

2010年发表论文列表（17篇）

- Jingzheng Wu, Yongji Wang, Liping Ding, Xiaofeng Liao. Improving Performance of Network Covert Timing Channel through Huffman Coding. The 2010 FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA 2010). Gwangju, Korea. Dec 9-11, 2010.
- Jingzheng Wu, Yongji Wang, Liping Ding, Yanping Zhang. Constructing Scenario of Event-Flag Covert Channel in Secure Operating System. 2nd International Conference on Information and Multimedia Technology (ICIMT 2010). Hongkong. Dec 28-30, 2010.
- Li Shang-Jie, He Ye-Ping. A Privacy-Preserving Integrity Measurement Architecture. Proceeding of Third International Symposium on Electronic Commerce and Security, 2010, Guangzhou, China, pp242-246.
- Li Shang-Jie, He Ye-Ping. On Property-based Attestation. The IASTED International Conference on Communication and Information Security, 2010,Marina Del Rey, USA.
- Li Shangjie, He Yeping. Trusted Subjects Configuration based on TE model in MLS Systems. 2nd International Conference of Trusted Systems(INTRUST 2010), 2010, Beijing, China.
- Tian Shuo, He Yeping, Ding Liping. A Countermeasure against Stack-smashing Attack Based on Canary Obtained through Nonlinear Transformation. Proceedings of 2010 2nd International Conference on Information and Multimedia Technology (ICIMT 2010), Hong Kong 12.28-12.30.2010
- Zhang Qian, He Yeping, Meng Ce. Towards Remote Attestation of Security Policies . In Proceedings of International Conference on Networks Security, Wireless Communications and Trusted Computing(NSWCTC2010), P475-478. Wuhan, China.
- Zhang Qian, He Yeping, Meng Ce. Semantic Remote Attestation for Security Policy. In Proceedings of International Conference on Information Science and Applications(ICISA 2010), P407-414. Seoul, Korea.
- 王永吉,吴敬征,曾海涛,丁丽萍,廖晓锋. 隐蔽信道研究. 软件学报, 2010,21(9):2262-2288. http://www.jos.org.cn/1000-9825/3880.htm
- Xiaofeng Liao; Yongji Wang, Liping Ding. A Novel Duplicate Images Detection Method Based on PLSA Model. 2010 3rd International Conference on Machine Vision (ICMV 2010). Hongkong. 2010.
- Xiaofeng Liao, Yongji Wang, Liping Ding. Discovering Temporal Patterns from Images using Extended PLSA. International Conference on Multimedia Technology. Ningbo, China; IEEE. 2010.
- Liping Ding, Gujian, Yongji Wang, Jingzheng Wu. Analysis of Telephone Call Detail Records Based on Fuzzy Decision Tree. Proceedings of ICST Conference on Forensics Applications and Techniques in Telecommunications , Information and Multimedia. Shanghai, 2010, China.
- [13] Yasen Aizezi, Liping Ding, Dilixiati Maimaiti, Qiong Wan . Research on the Helper of EnCase for Digital Evidences in Uyghur-Kazak-Kyrgyz. Analysis of Telephone Call Detail Records Based on Fuzzy Decision Tree. Proceedings of ICST Conference on Forensics Applications and Techniques in Telecommunications , Information and Multimedia. Shanghai, 2010, China.
- 蒋建春，文伟平.“云”计算环境的信息安全问题.《信息网络安全》. 2010年2期.
- Jianchun Jiang, Weifeng Chen, Liping Ding. "On Estimating Cyber Adversaries' Capabilities - A Bayesian Model Approach". (Poster) Proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection (RAID 2010), Ottawa, Canada, September 15-17, 2010.
- 陈超，蒋建春，丁治明.基于时序片段评价的数据分配算法。计算机研究与发展。第47卷，增刊，2010年10月。
- Weifeng Chen, Jianchun Jiang, and Nancy Skocik. "On the Privacy Protection in Publish/Subscribe Systems". Proceedings of IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS2010), Beijing, China, June 25-27, 2010.

中国科学院软件研究所
基础软件国家工程研究中心
National Engineering Research Center of Fundamental Software
Institute of Software, Chinese Academy of Sciences

2011年阶段性成果

- Liping Ding, Yifei Guo, Jian Gu and Jingzheng Wu. DRMIBT: a New DRM Implementation Based on Virtual Machine. 2011 International Conference on Information and Industrial Electronics (ICIIE 2011). Chengdu. Jan 14-15, 2011.
- Jingzheng Wu, Yongji Wang, Liping Ding, Wei Han. A Practical Covert Channel Identification Approach in Source Code based on Directed Information Flow Graph. The Fifth Annual International Conference on Secure Software Integration and Reliability Improvement (SSIRI 2011). Jeju Island, Korea. Jun 27-29, 2011: (Accepted).
- Xiaofeng Liao, Liping Ding,Yongji Wang. Secure Machine Learning, A Brief Overview. The Fifth Annual International Conference on Secure Software Integration and Reliability Improvement (SSIRI 2011). Jeju Island, Korea. Jun 27-29, 2011: (Accepted).
- Wei Han, Yeping He, Liping Ding. Verifying the Safety of Xen Security Modules. The Fifth Annual International Conference on Secure Software Integration and Reliability Improvement (SSIRI 2011). Jeju Island, Korea. Jun 27-29, 2011: (Accepted).
- Ennan Zhaiy, Liping Dingy, Sihan Qingy;z. Towards a Reliable Spam-Proof Tagging System. The Fifth Annual International Conference on Secure Software Integration and Reliability Improvement (SSIRI 2011). Jeju Island, Korea. Jun 27-29, 2011: (Accepted).
- Jingzheng Wu, Yongji Wang, Liping Ding, Wei Han. Identification and Evaluation of Sharing Memory Covert Timing Channel in Xen Virtual Machines. IEEE 4th International Conference on Cloud Computing (CLOUD 2011). Washington DC, USA. July 4-9, 2011:(Accepted).
- Ming Li, Liping Ding, Shuo Tian. Analysis and Research on Security Defense Strategies of Cloud Security. ICETC 2011, July 15 - 16, 2011, Changchun, China: (Accepted).

云计算隐蔽信道分析的工业价值

- 云计算掀起了当今IT业的又一次研究热潮，产业界对云计算能够带来的实际效益更加注重。然而，云安全是制约云计算发展的瓶颈。如何隔离用户数据，保证数据的机密性、完整性以及可用性将会是今后工业界的研究重点，也是解决云安全问题的关键。

谢谢大家，请批评指正!

中国科学院软件研究所
基础软件国家工程研究中心
National Engineering Research Center of Fundamental Software
Institute of Software, Chinese Academy of Sciences