云环境软件可信状态探测机制

石文昌 教授
中国人民大学 信息学院
wenchang@ruc.edu.cn

报告大纲

一．问题与思路
二．国际相关工作
三．已开展的工作
四．关键技术

报告大纲

一．问题与思路

二．国际相关工作

三．已开展的工作

四．关键技术

云环境的可信状况

- 服务提供者安全举措透明度的不足削弱了用户对云系统的信任。
- 加拿大联邦法律限制医疗卫生等敏感数据只能存储在加拿大领土内的机器上。
- 美国政府的监控行为促使人们对采用云服务持更为谨慎的态度，尤其在欧洲。

M. Nanavati, P. Colp, W. Aiello, A. Warfield. Cloud Security: A Gathering Storm. Communications of the ACM, 57(5), May 2014: 70-79.

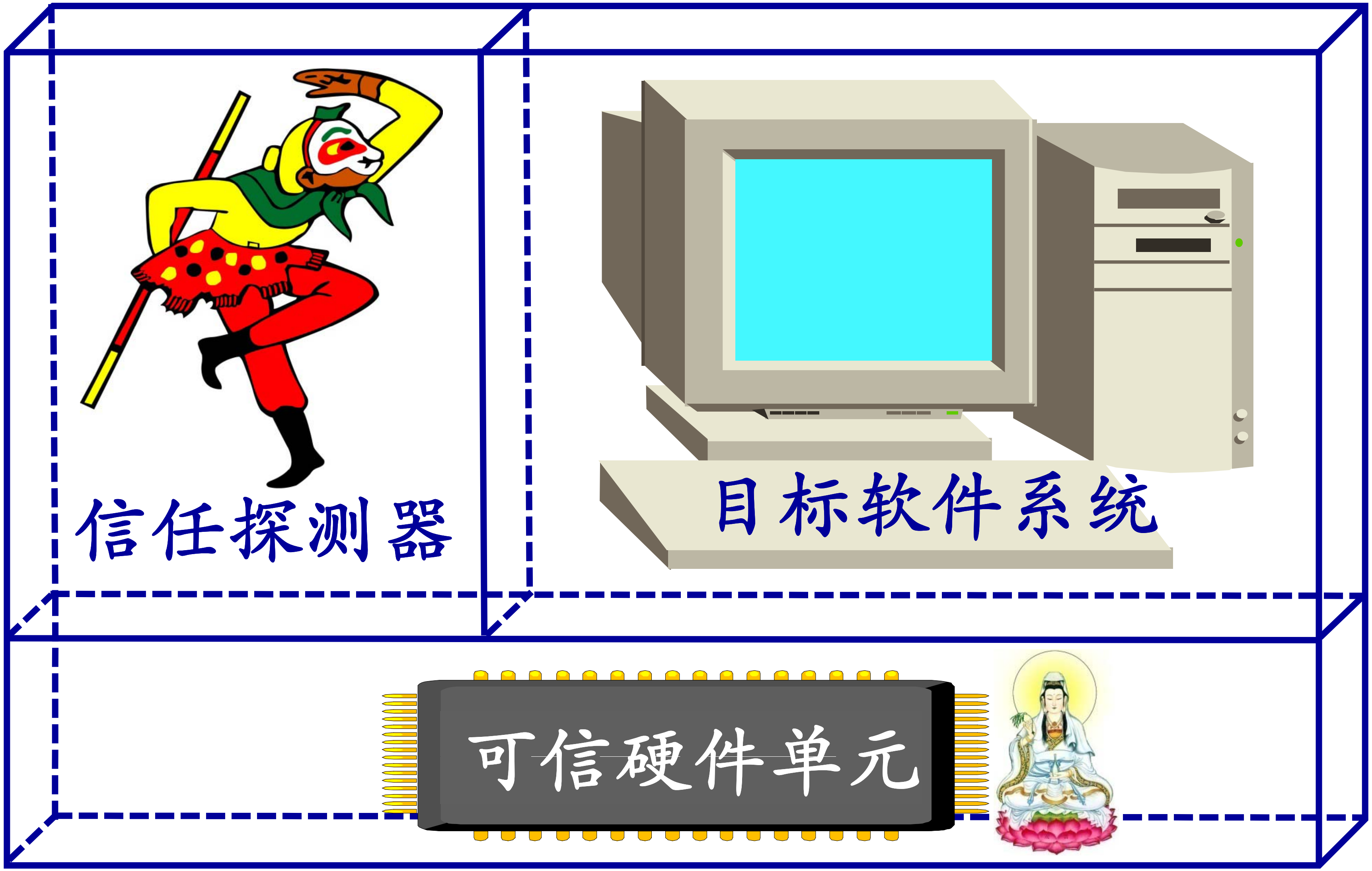
问题

如何弄清

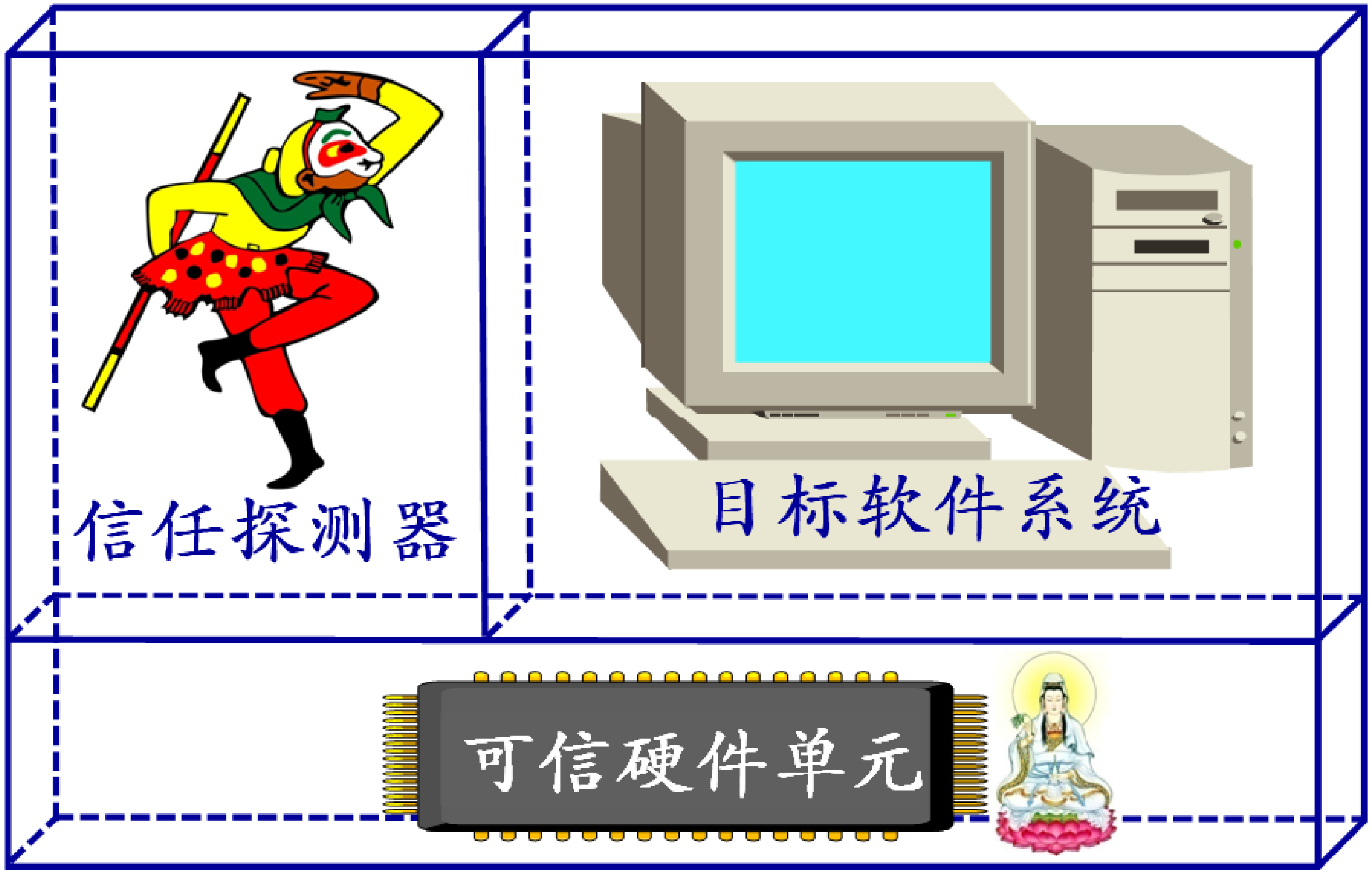
云计算环境的可信状况

？？？

软件信任探测器思想



软件信任探测器思想

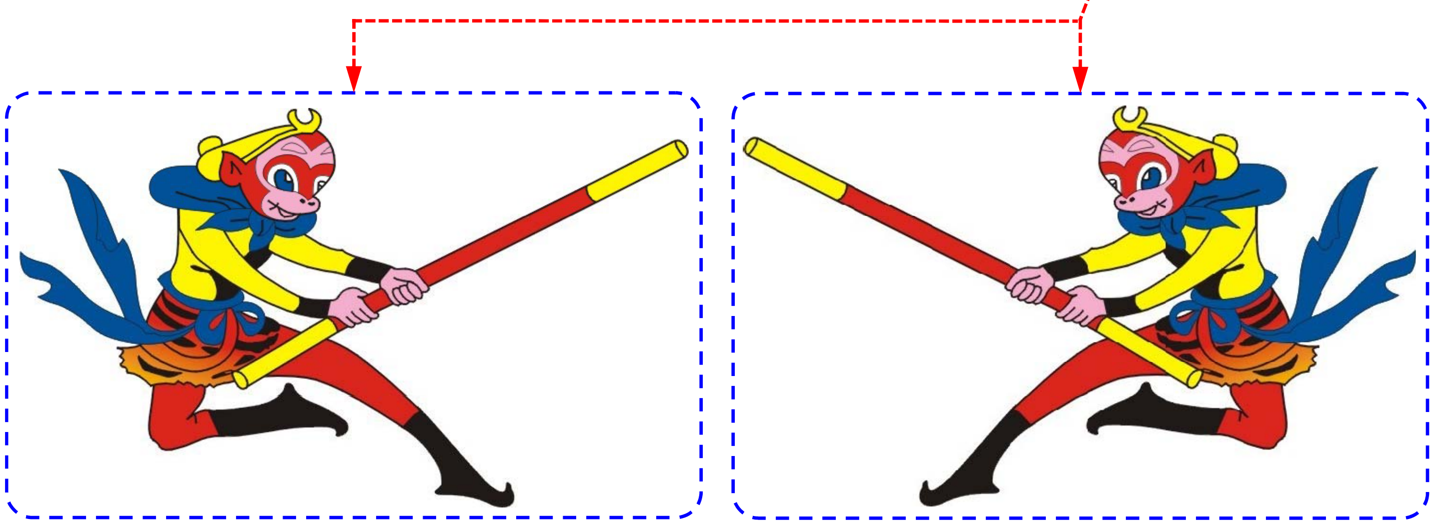


W.C. Shi, "*On Design of Trusted Software Base with Support of TPCM*," INTRUST 2009, LNCS 6163, Springer-Verlag, pp.1-15, 2010.

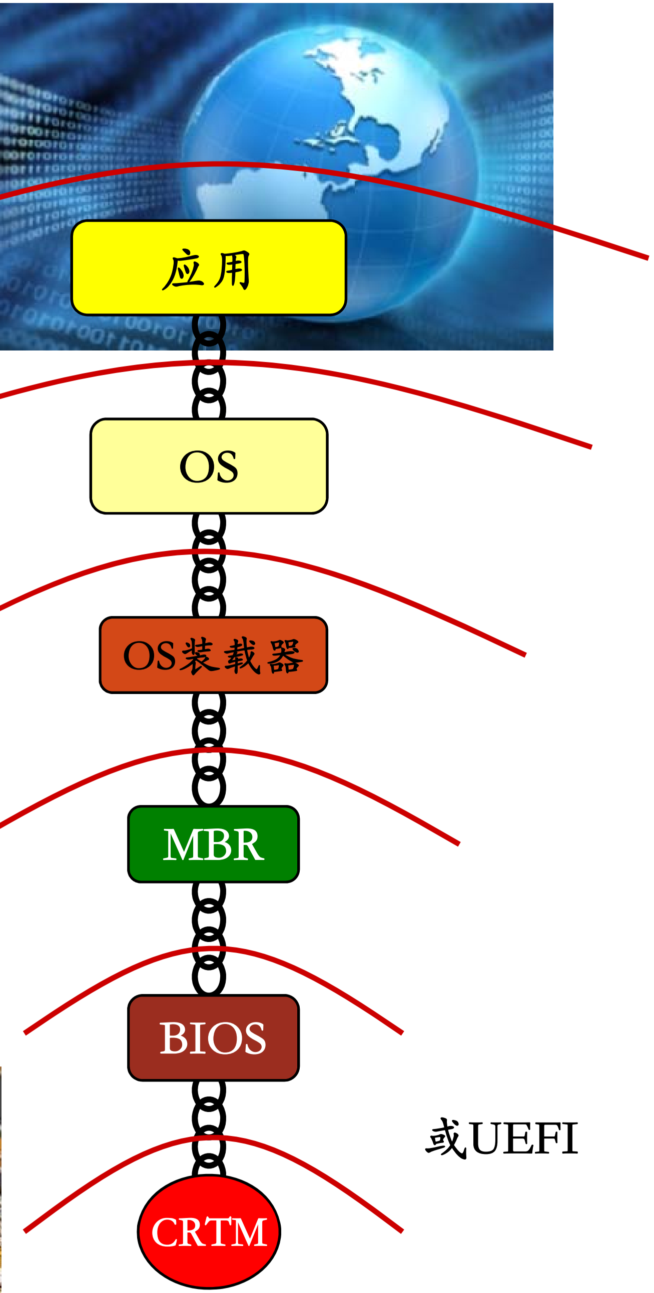
需要解决的问题

一．如何测定目标软件系统的可信状态？

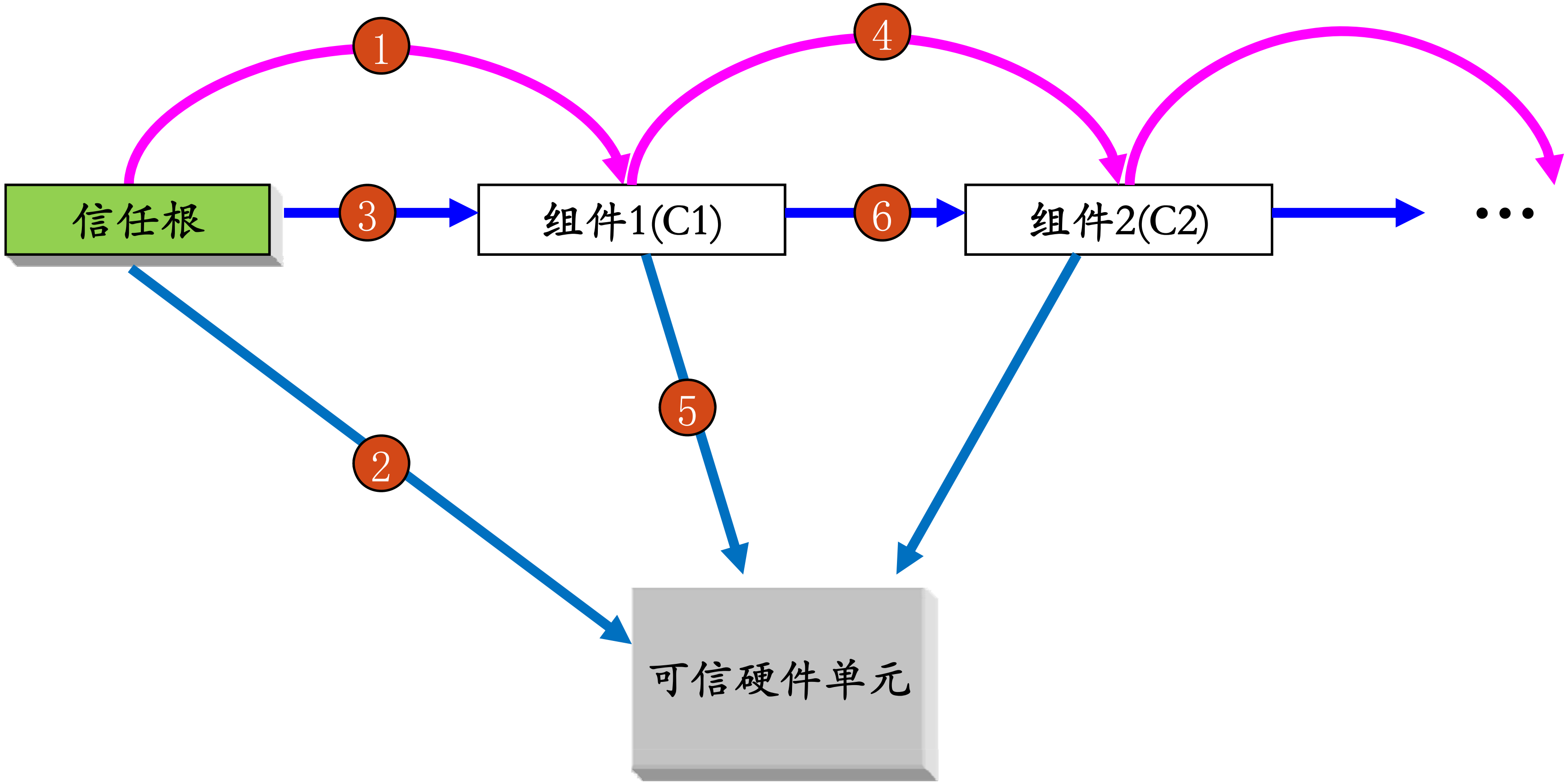
二．如何确保探测器的可信？



探测器支撑架构



信任传递思想



报告大纲

一. 问题与思路
二. 国际相关工作
三. 已开展的工作
四. 关键技术

TCB：可信计算基的提出

SPECIFICATION OF A TRUSTED COMPUTING BASE (TCB)

THE MITRE CORPORATION
Bedford, Massachusetts

G. H. Nibaldi

30 November 1979

A Trusted Computing Base (TCB) is the totality of access control mechanisms for an operating system. A TCB should provide both a basic protection environment and the additional user services required for a trustworthy turnkey system. The basic protection environment is equivalent to that provided by a security kernel; the user services are analogous to the facilities provided by trusted processes in kernel-based systems. This report documents the performance, design, and development requirements for a TCB for a general-purpose operating system.

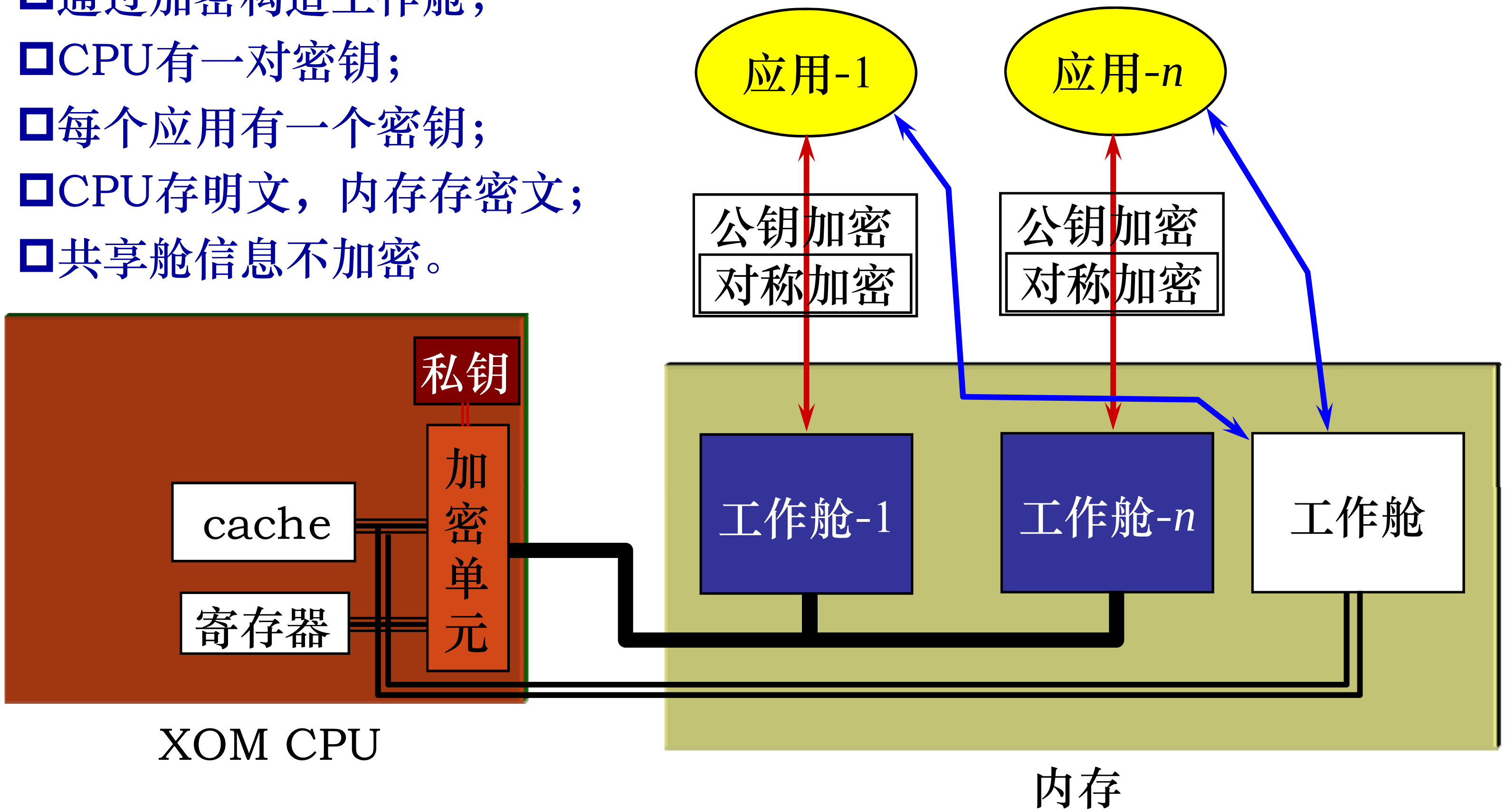
什么是可信计算基？

- A TCB is the totality of access control mechanisms for an operating system.
- A TCB is a hardware and software access control mechanism
    - that establishes a protection environment to control the sharing of information in computer systems.
- A TCB is an implementation of a reference monitor
    - that controls when and how data is accessed.

多伦多大学
微软
斯坦福大学

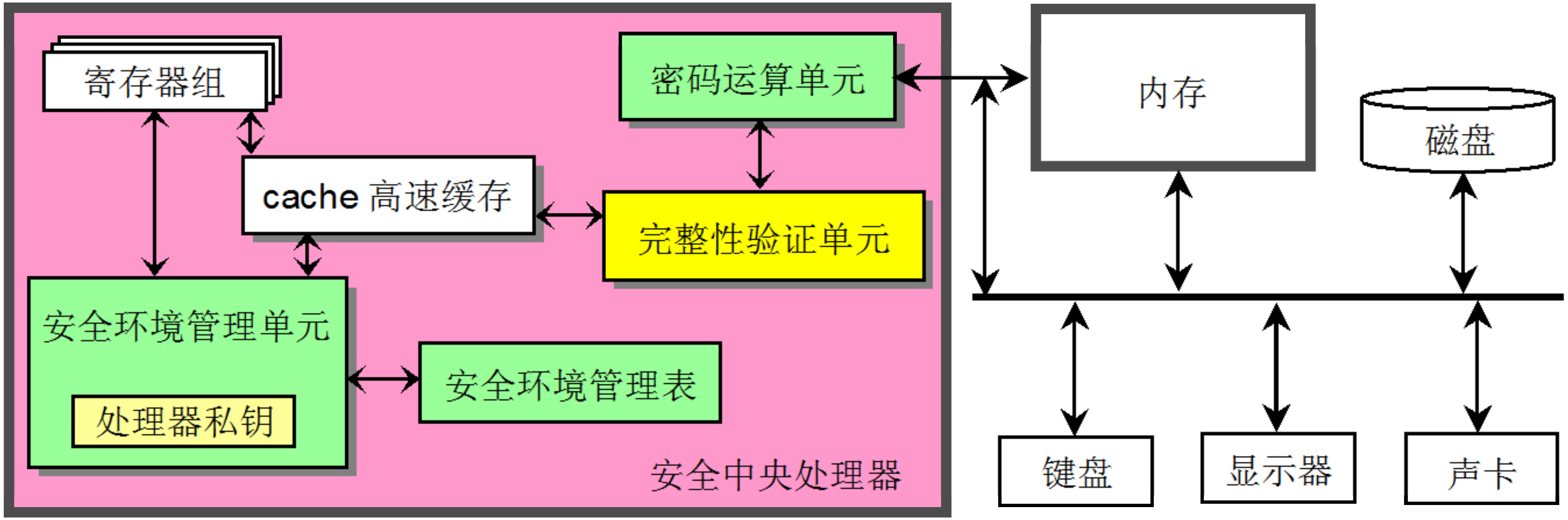
XOM安全模型体系架构

- 通过加密构造工作舱；
- CPU有一对密钥；
- 每个应用有一个密钥；
- CPU存明文，内存存密文；
- 共享舱信息不加密。



D. Lie, C.A. Thekkath, M. Horowitz. Implementing an Untrusted Operating System on Trusted Hardware. ACM SIGOPS Operating Systems Review, 37(5), Dec 2003:178~192.

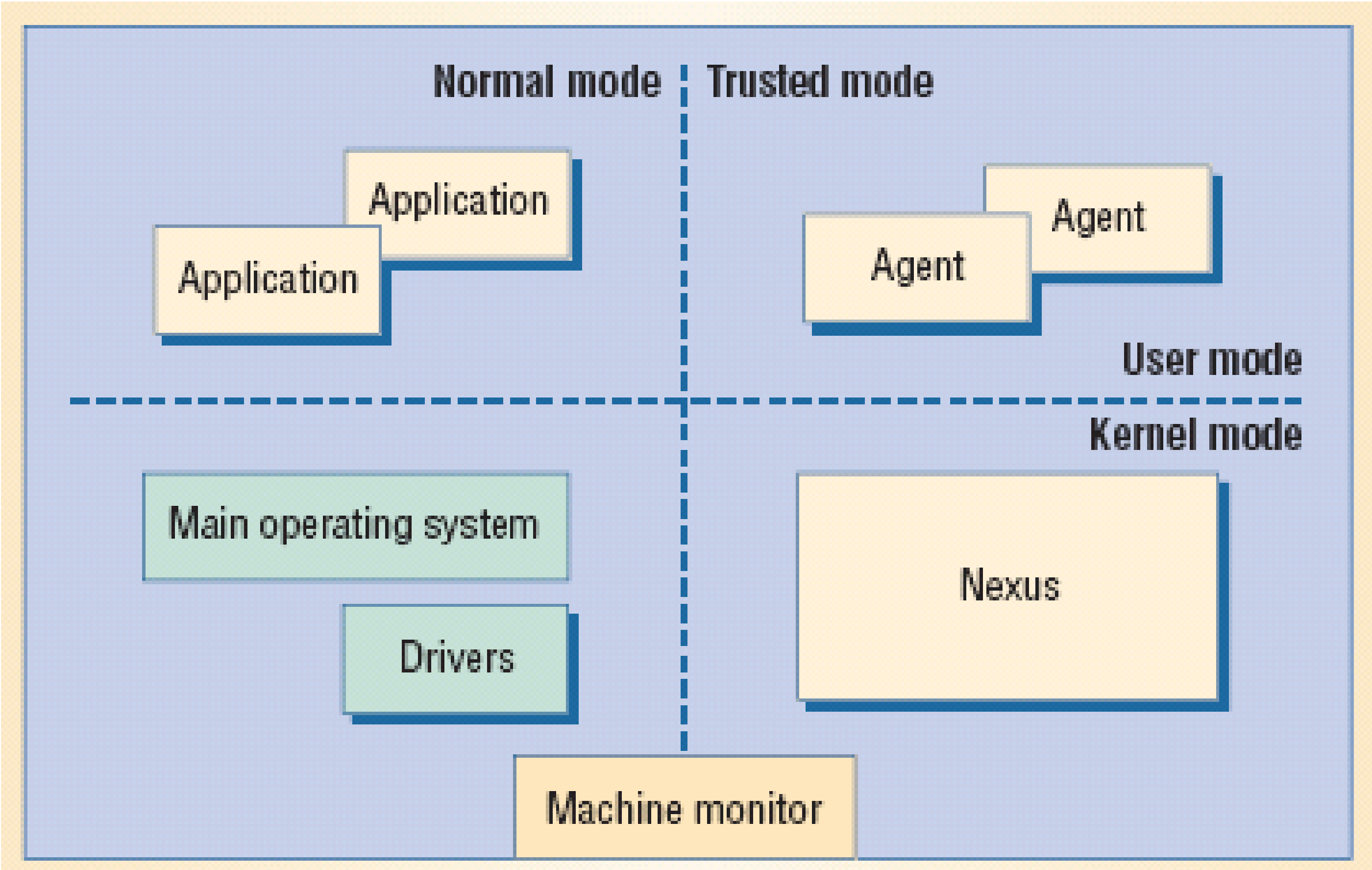
AEGIS安全模型体系架构



- 添加的安全支持单元：
  - 密码运算单元
  - 完整性验证单元

G.E. Suh, D. Clarke, B. Gassend, M. van Dijk, S. Devadas. AEGIS: Architecture for Tamper-Evident and Tamper-Resistant Processing. Proceedings of the 17th Annual International Conference on Supercomputing (ICS'03), ACM Press, 2003:160~171.

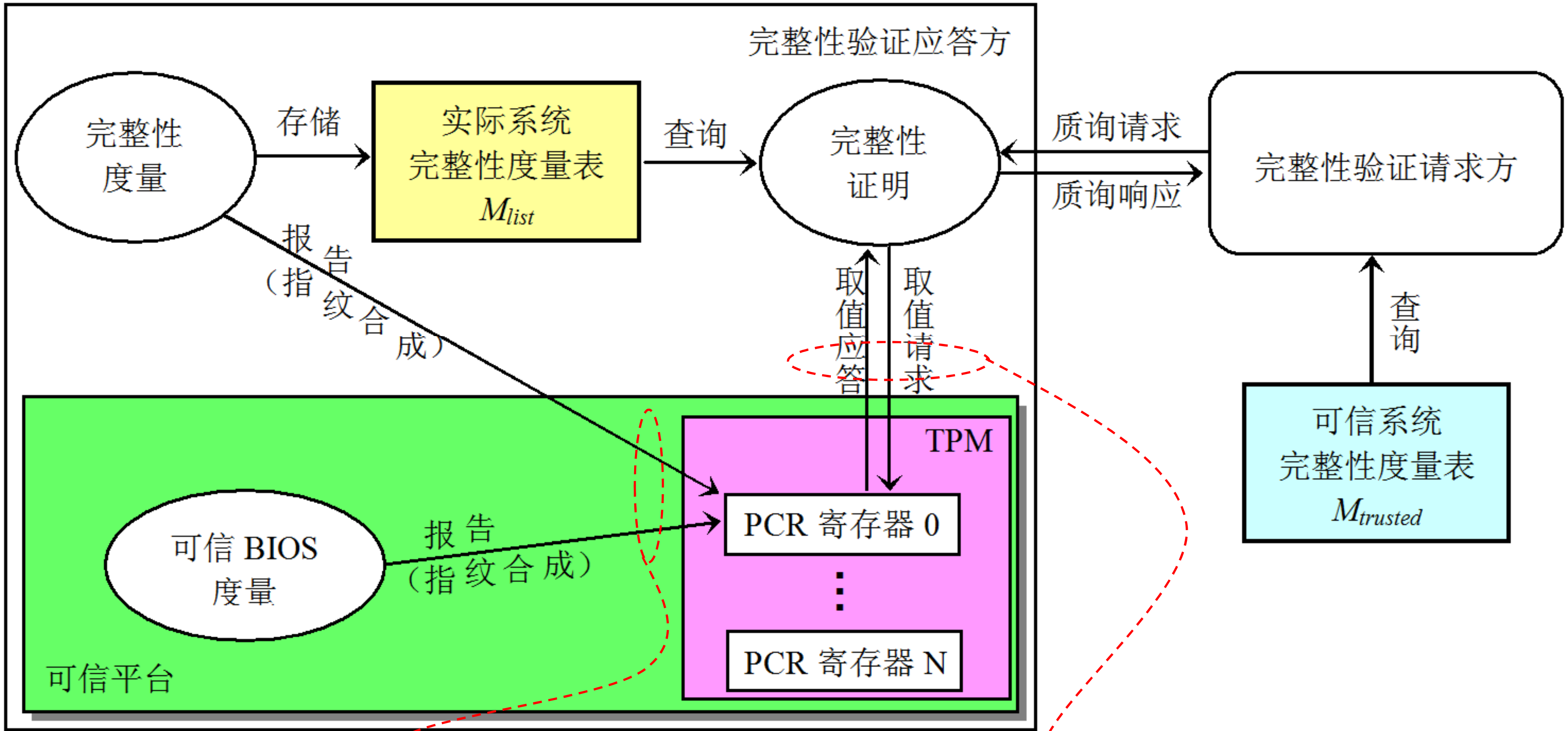
微软的NGSCB可信模型



P. England, B. Lampson, J. Manferdelli, M. Peinado, B. Willman. A Trusted Open Platform. IEEE Computer, 36(7), pp. 55-62. Jul 2003.

IBM沃森研究中心

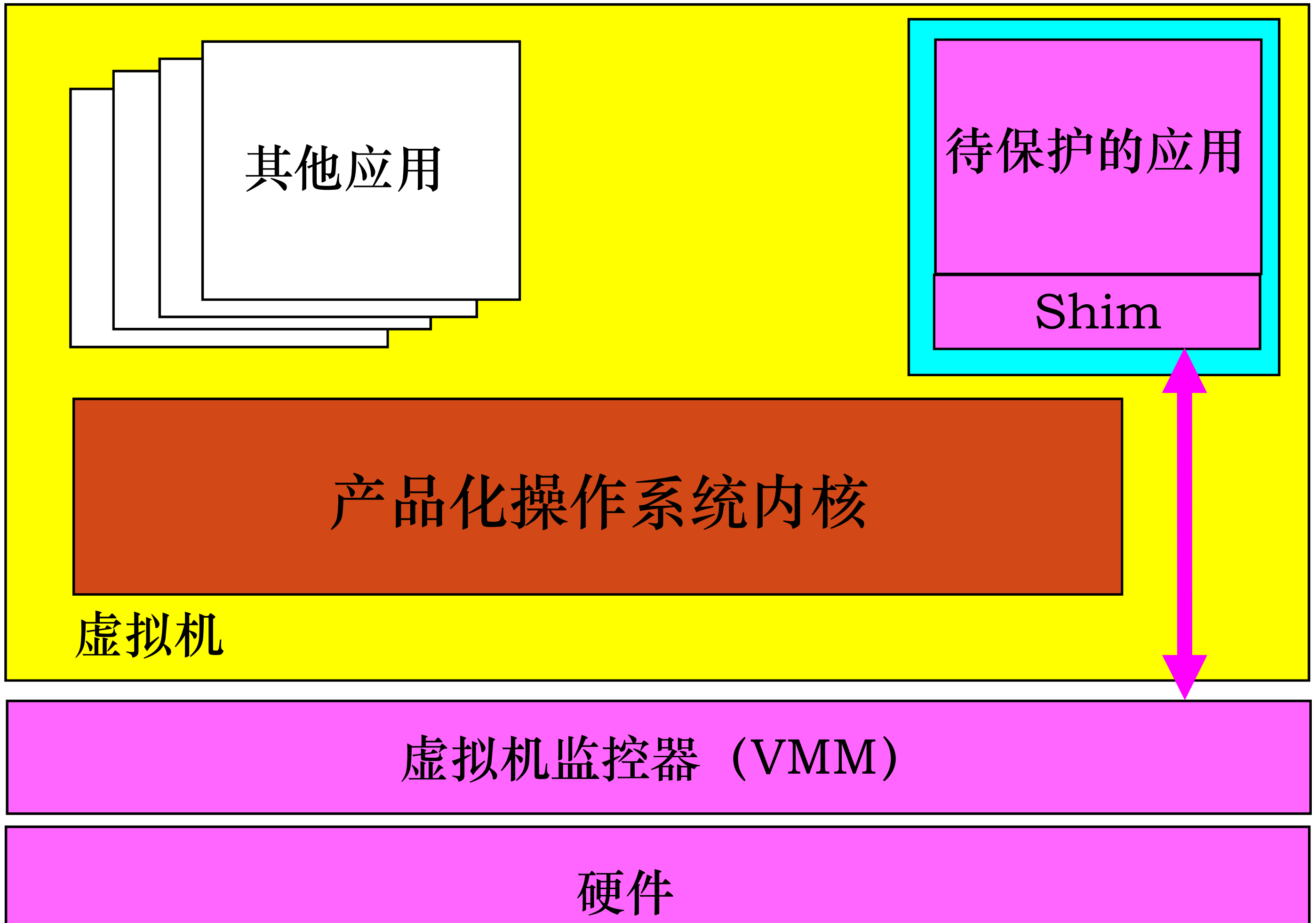
IMA信任体系架构



R. Sailer, X. Zhang, T. Jaeger, L. Van Doorn. Design and Implementation of a TCG-based Integrity Measurement Architecture. Proceedings of the 13th USENIX Security Symposium, San Diego, CA, USA, Aug. 2004: 223~238.

麻省理工学院
VMWare

基于Overshadow的应用安全方案



Dan R.K. Ports, Tal Garfinkel. Towards Application Security on Untrusted Operating Systems. 3rd USENIX Workshop on Hot Topics in Security (HotSec'08), San Jose, CA, USA, Jul 2008.

MITRE的对外证明体系结构

MTR080072

MITRE TECHNICAL REPORT

Attestation: Evidence and Trust

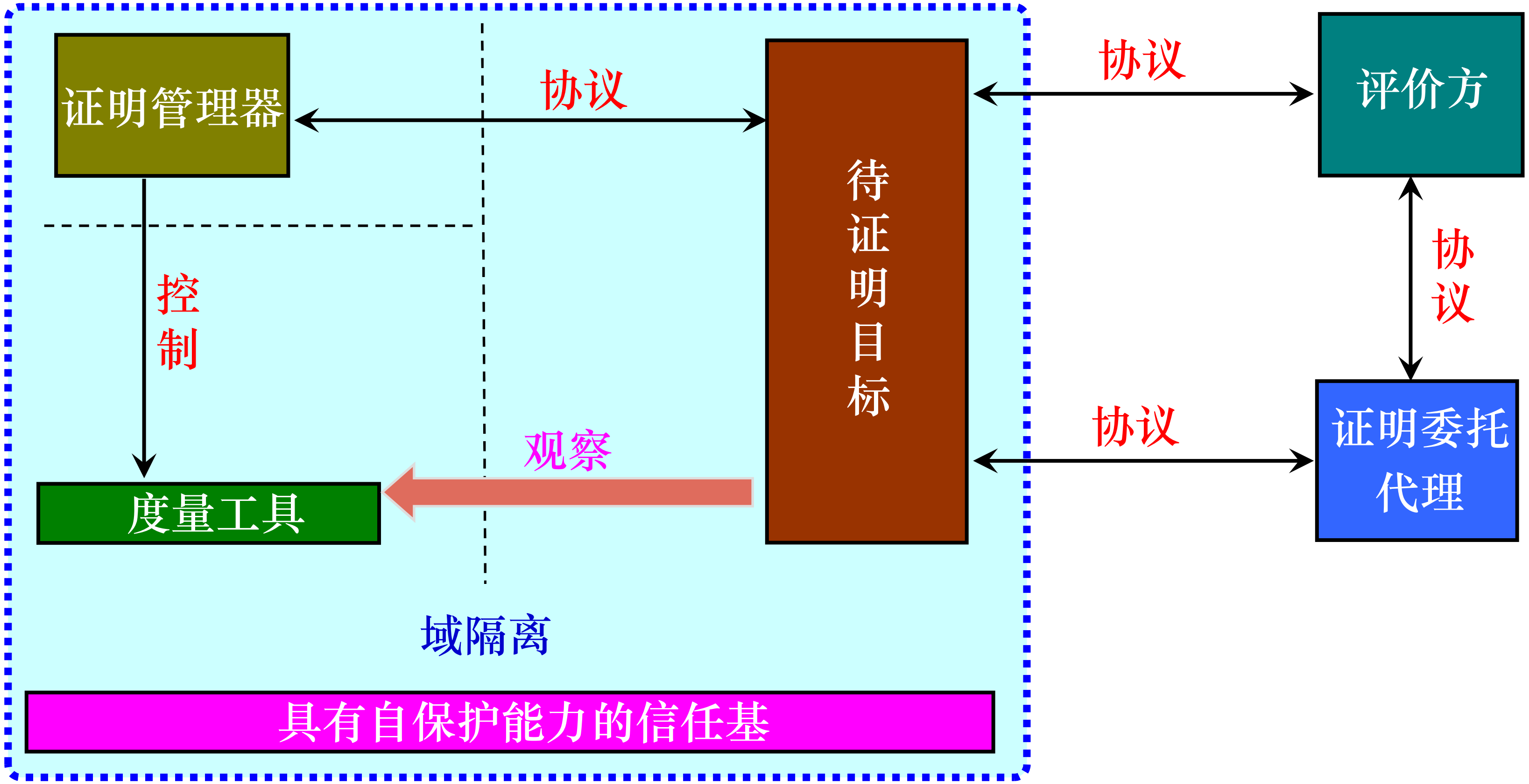
MITRE is a not-for-profit company that runs six US Government "Federally Funded Research & Development Centers" (FFRDCs) dedicated to working in the public interest. It is the manager for a number of standards such as CVE, CWE, OVAL, CAPEC, STIX, TAXI, etc.

March 2008

MITRE

Center for Integrated Intelligence Systems
Bedford, Massachusetts

MITRE的对外证明体系结构

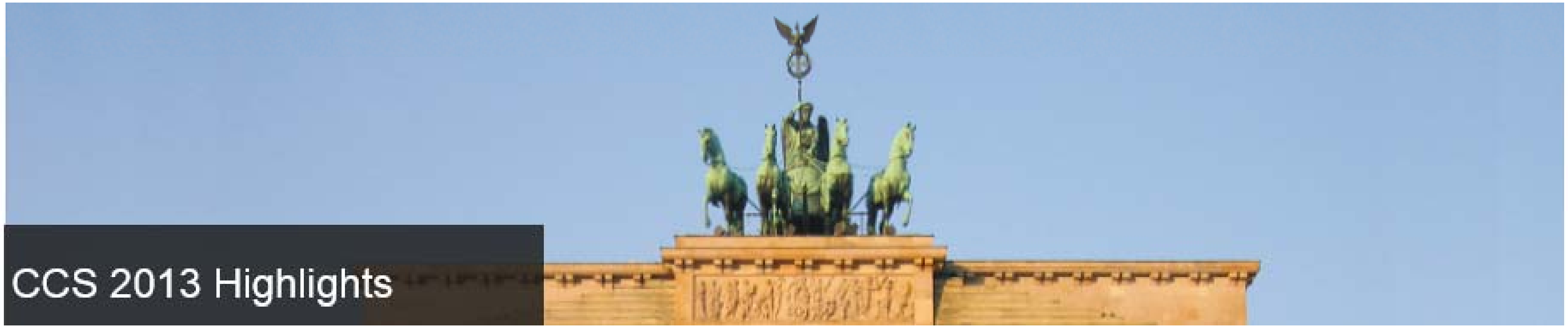


最新相关研究成果

acm SIGSAC

20th ACM Conference on Computer and Communications Security

November 4 - 8, 2013 Berlin, Germany



F. Armknecht, A.-R. Sadeghi, S. Schulz, C. Wachsmann. A Security Framework for the Analysis and Design of Software Attestation. 20th ACM Conference on Computer and Communications Security (CCS 2013), ACM Press, 2013:1~12.

E. Owusu, J. Guajardo, J. McCune, J. Newsome, A. Perrig, A. Vasudevan. OASIS: On Achieving a Sanctuary for Integrity and Secrecy on Untrusted Platforms. 20th ACM Conference on Computer and Communications Security (CCS 2013), ACM Press, 2013:13~24.

J. Butterworth, C. Kallenberg, X. Kovah, A. Herzog. BIOS Chronomancy: Fixing the Core Root of Trust for Measurement. 20th ACM Conference on Computer and Communications Security (CCS 2013), ACM Press, 2013:25~36.

报告大纲

一．问题与思路

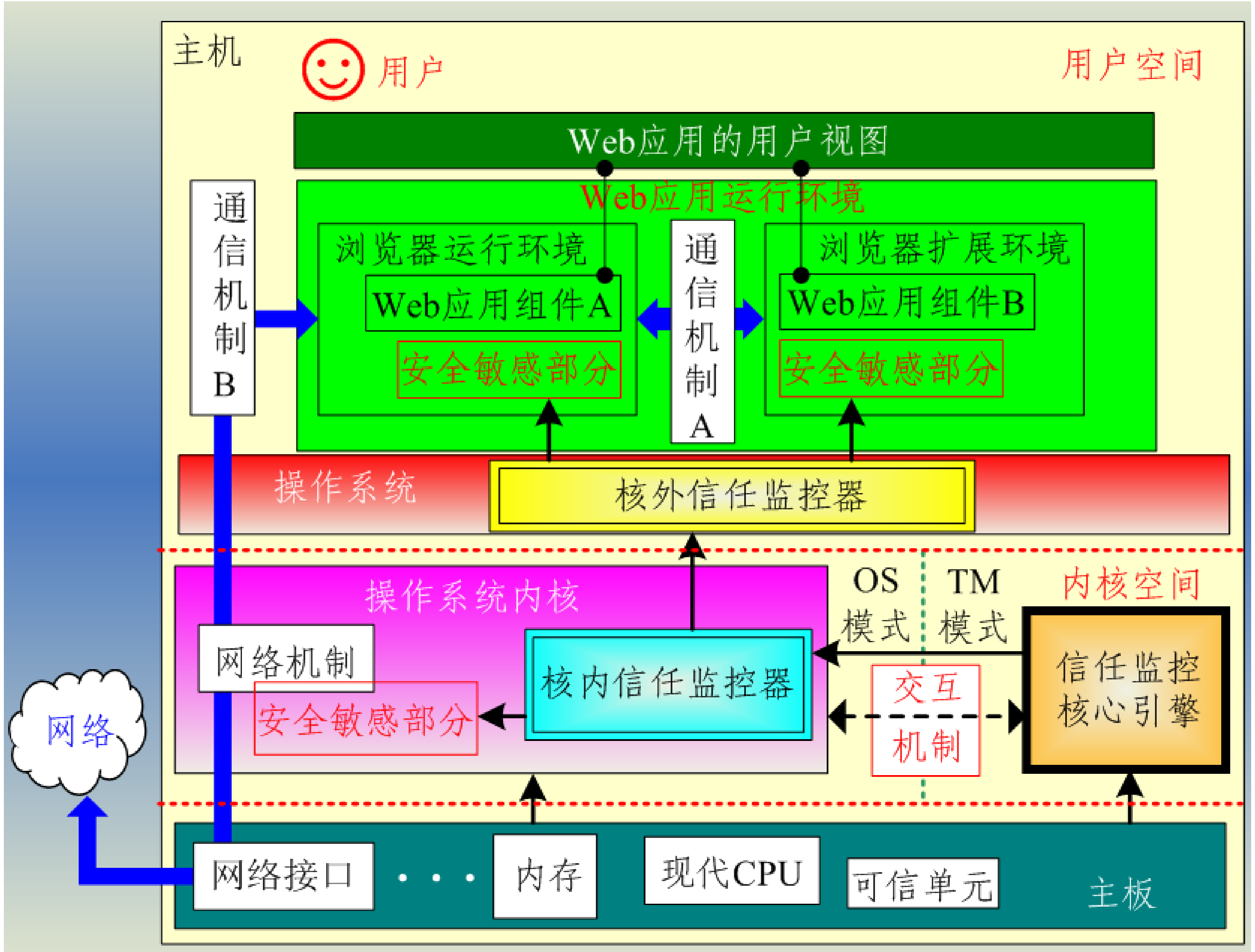
二．国际相关工作

三．已开展的工作

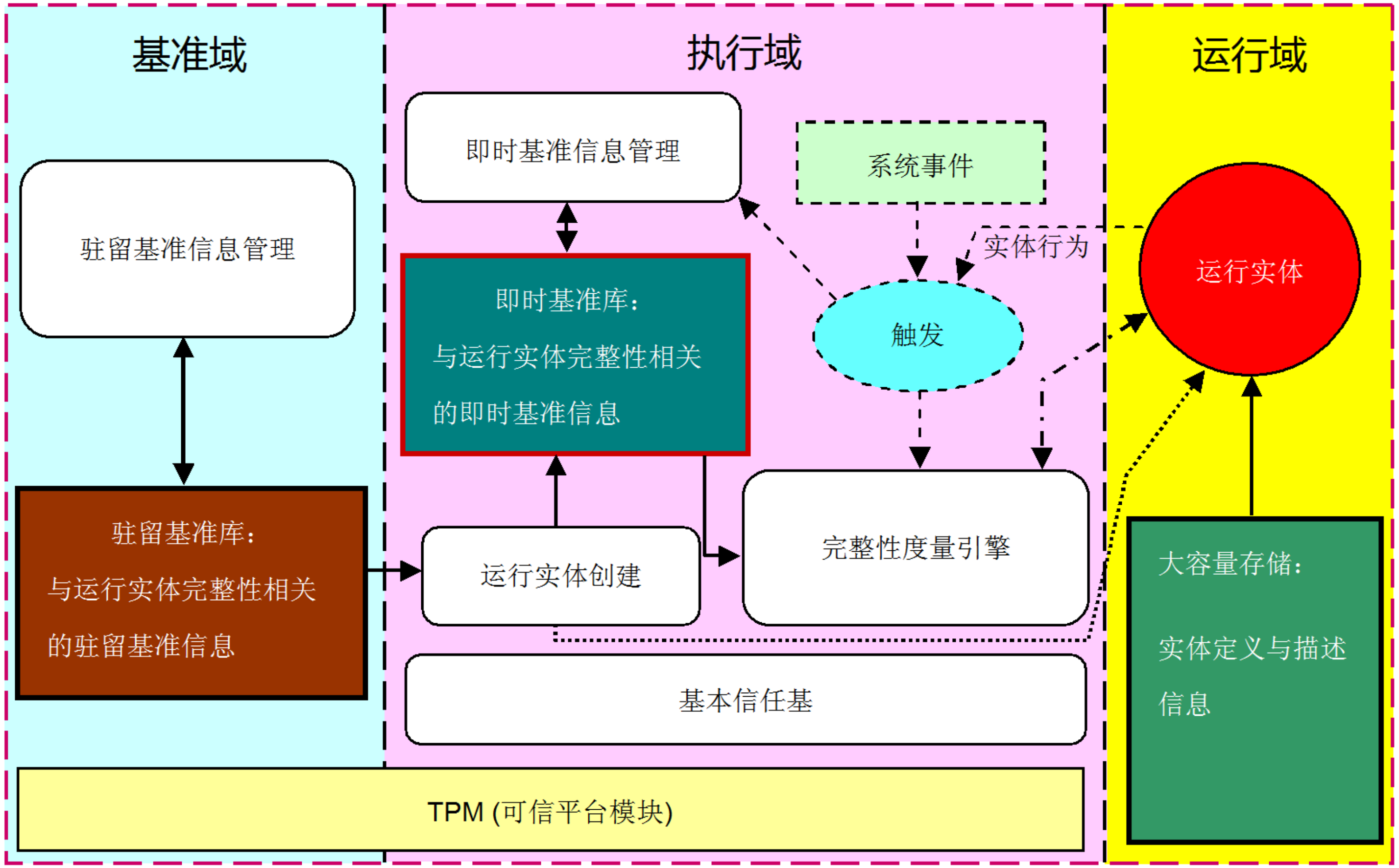
四．关键技术

探测器的构造原理

Web客户端的信任探测器

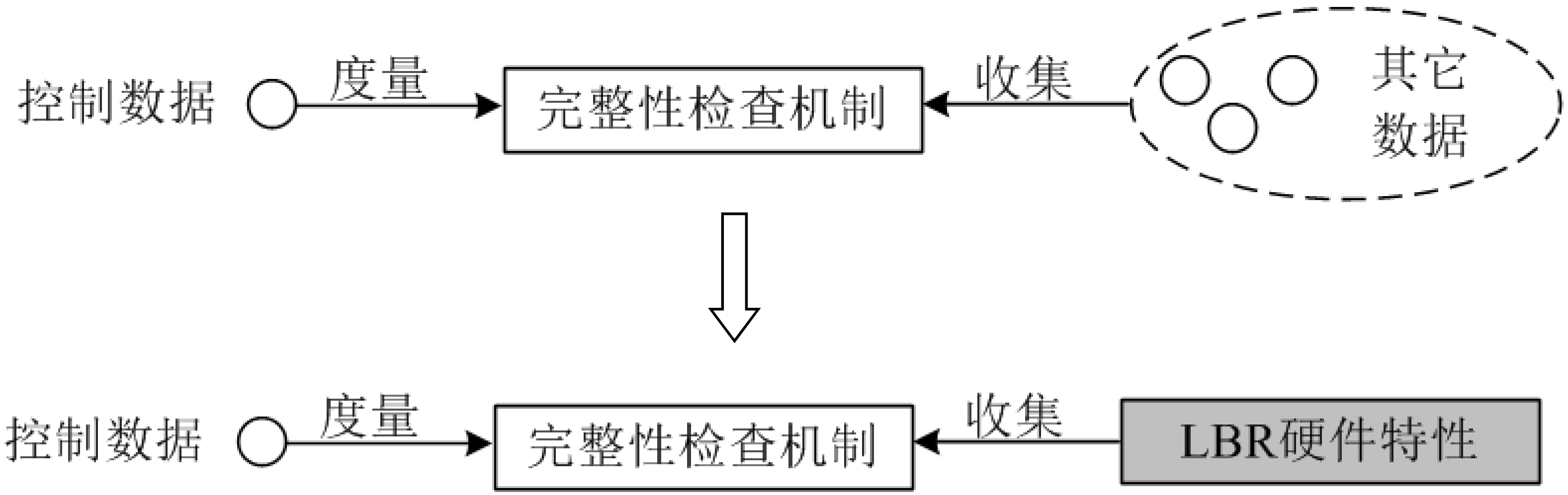


可信评判1：检测进程完整性



X. Li, W.C. Shi, Z.H. Liang, B. Liang, Z.Y. Shan, "*Operating System Mechanisms for TPM-Based Lifetime Measurement of Process Integrity*," IEEE MASS 2009 & TSP 2009, IEEE Computer Society, pp. 783-789, 2009.

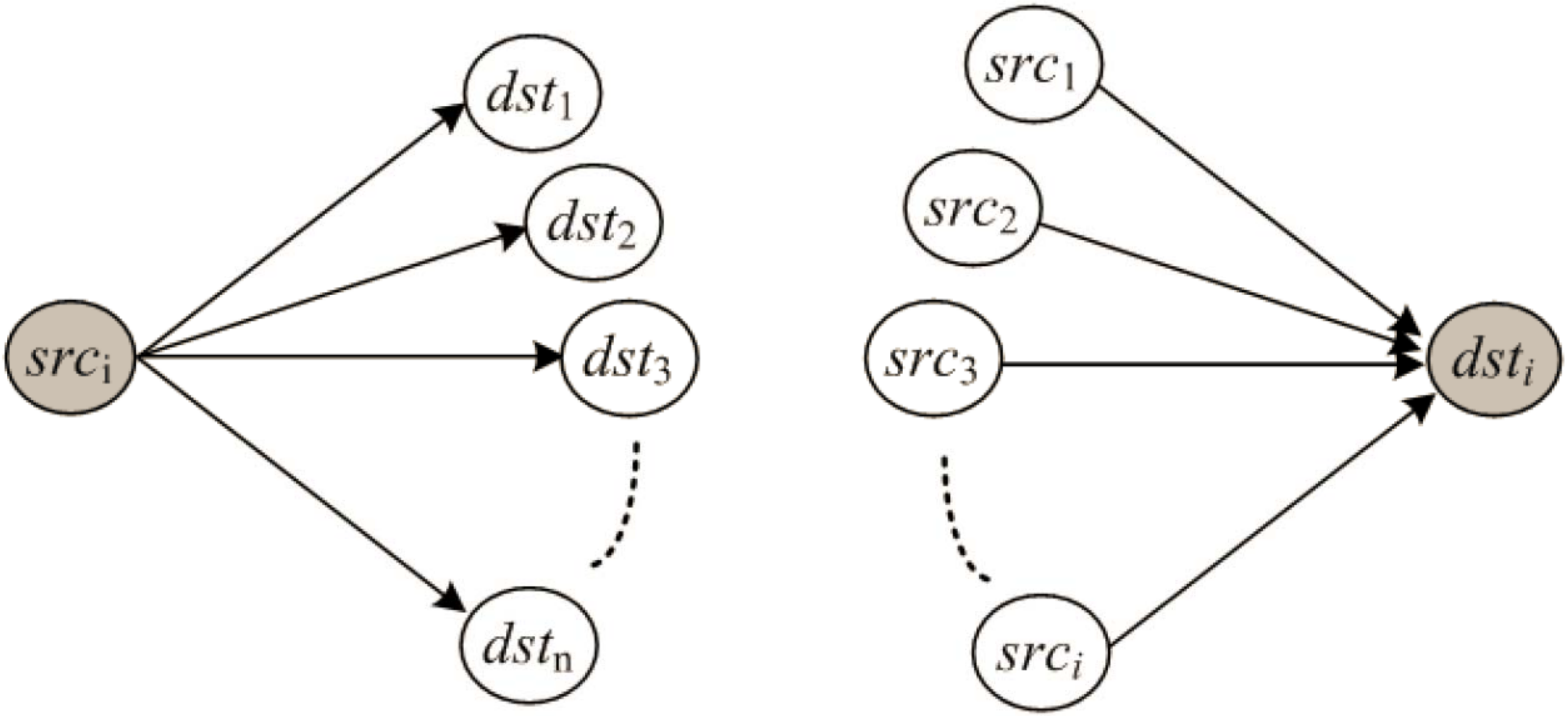
可信评判2：检测控制数据完整性



LBR（Late Branch Record）的主要功能：记录CPU最近执行的若干控制转移指令的基本信息。

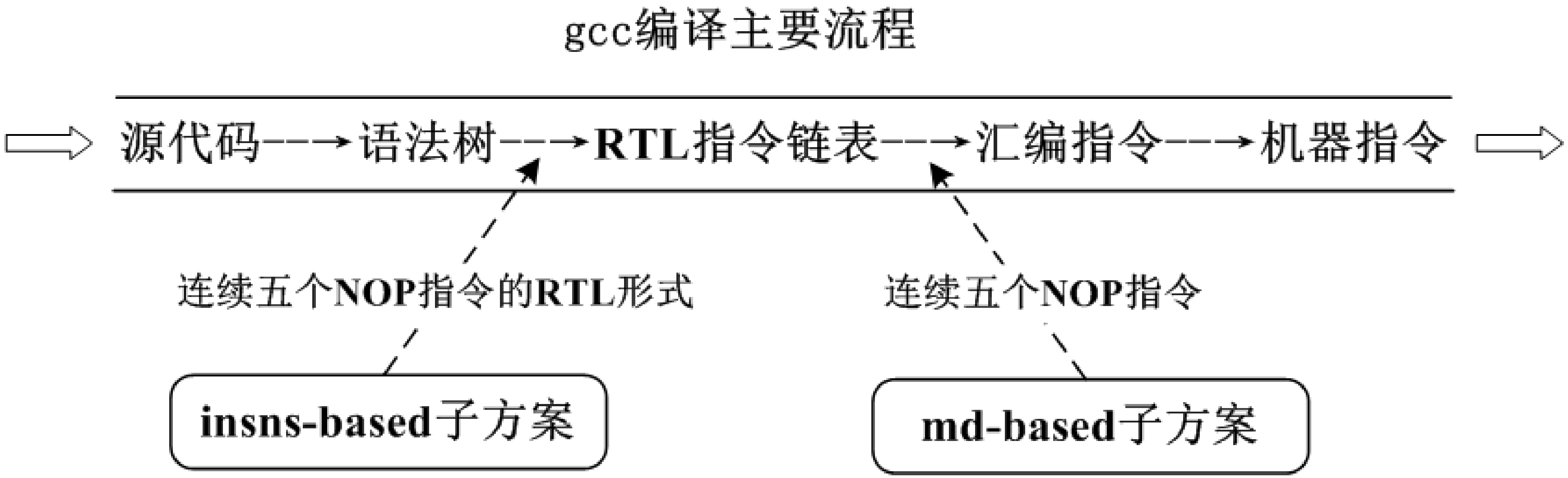
W.C. Shi, H.W. Zhou, J.H. Yuan, B. Liang, “*Detecting Compromised Kernel Hooks with Support of Hardware Debugging Features*,” China Communications, 9(10), pp. 78-90, 2012.

控制数据完整性检测原理

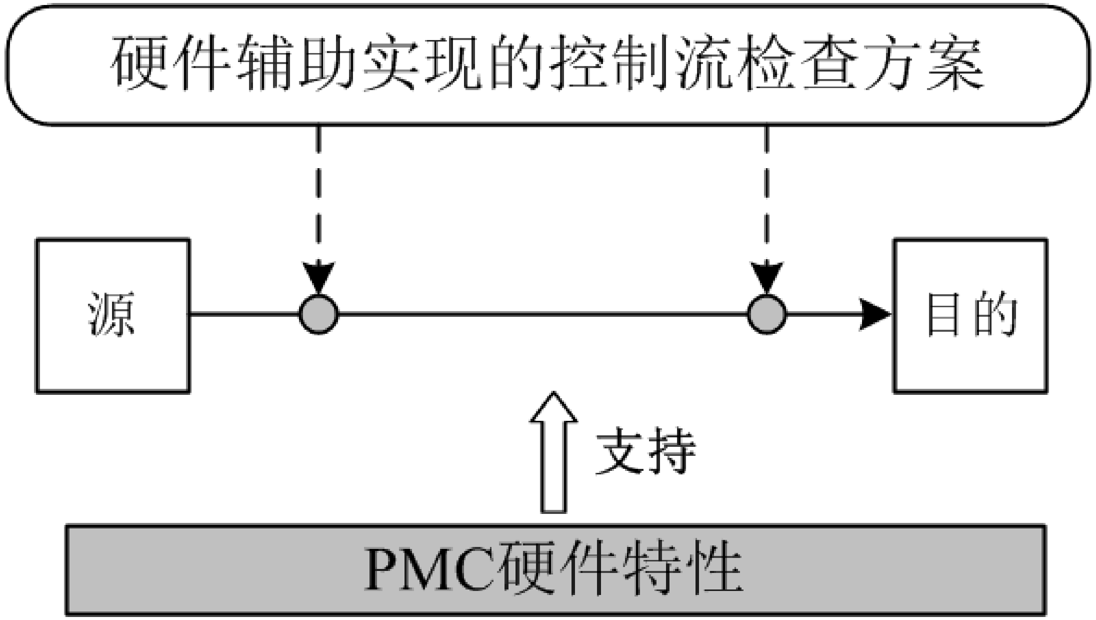


探针部署措施

- 扩展gcc编译器



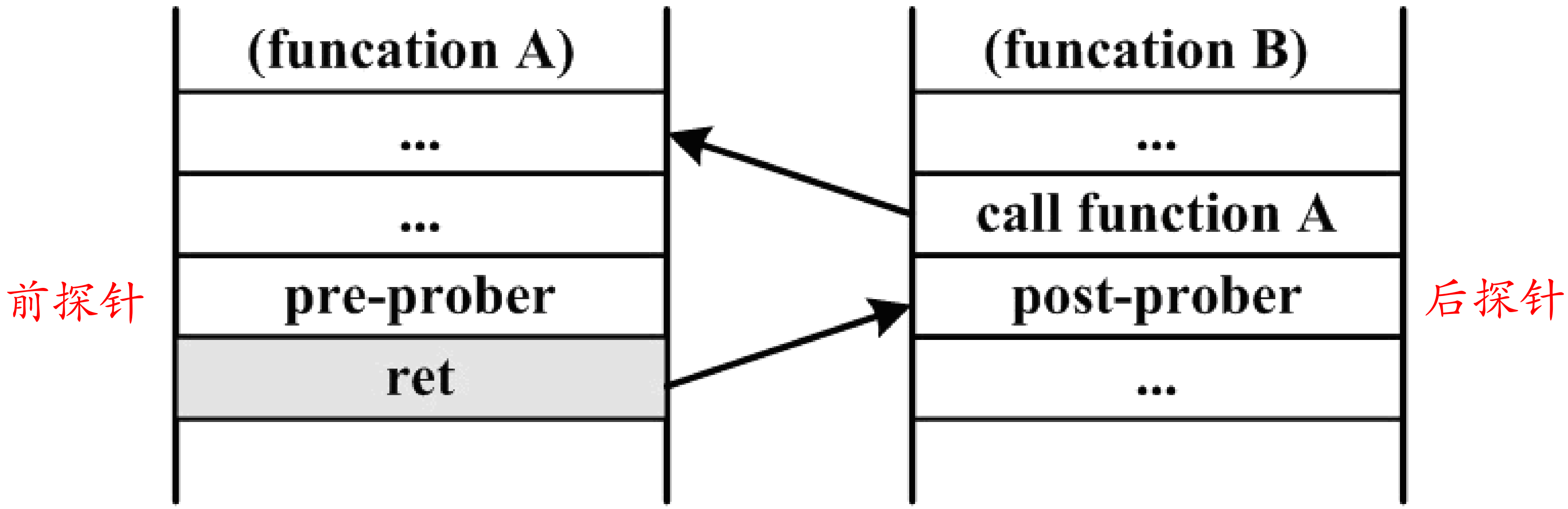
可信评判3：检测控制流完整性



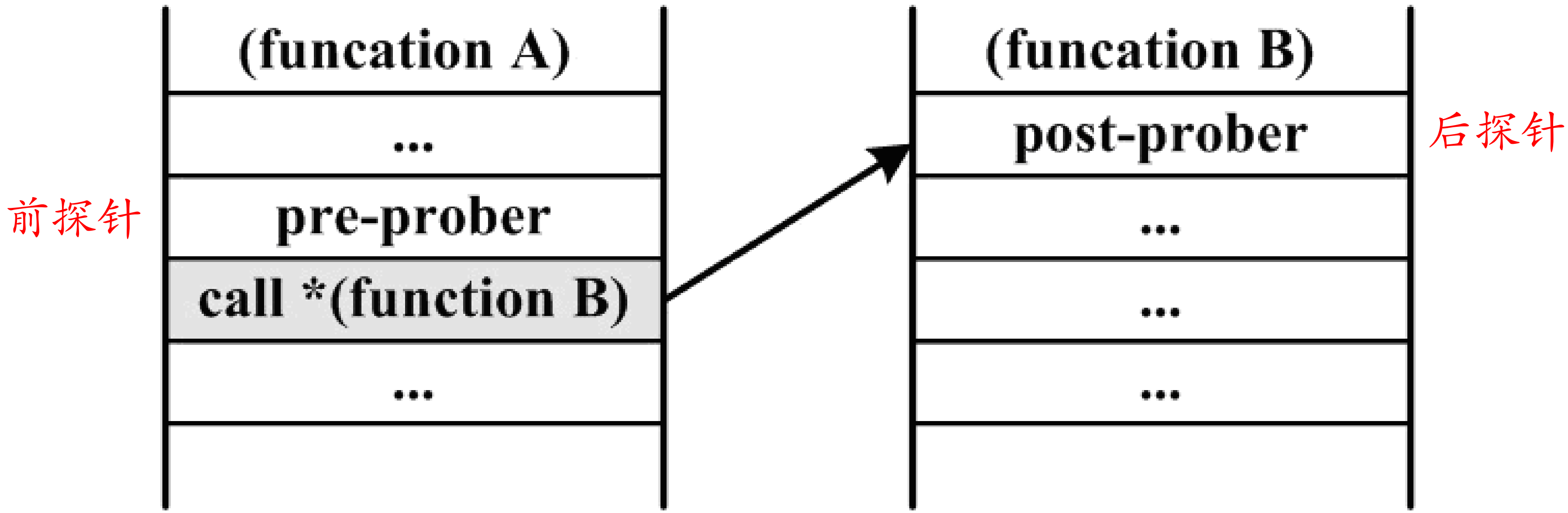
PMC（Performance Monitoring Counter）的主要功能：记录CPU中事件发生次数，典型事件记录：控制转移执行次数、控制转移预测成功/失败次数。

W.C. Shi, H.W. Zhou, J.H. Yuan, B. Liang, "*DCFI-Checker: Checking Kernel Dynamic Control Flow Integrity with Performance Monitoring Counter*," China Communications, 11(9), pp. 31-46, 2014.

RET指令探针部署


(funcation A)
...
...
前探针
pre-prober
ret
(funcation B)
...
call function A
post-prober
后探针
...

间接跳转指令探针部署


前探针
(funcation A)
...
pre-prober
call *(function B)
...
(funcation B)
post-prober
后探针
...
...
...

控制流完整性检测算法

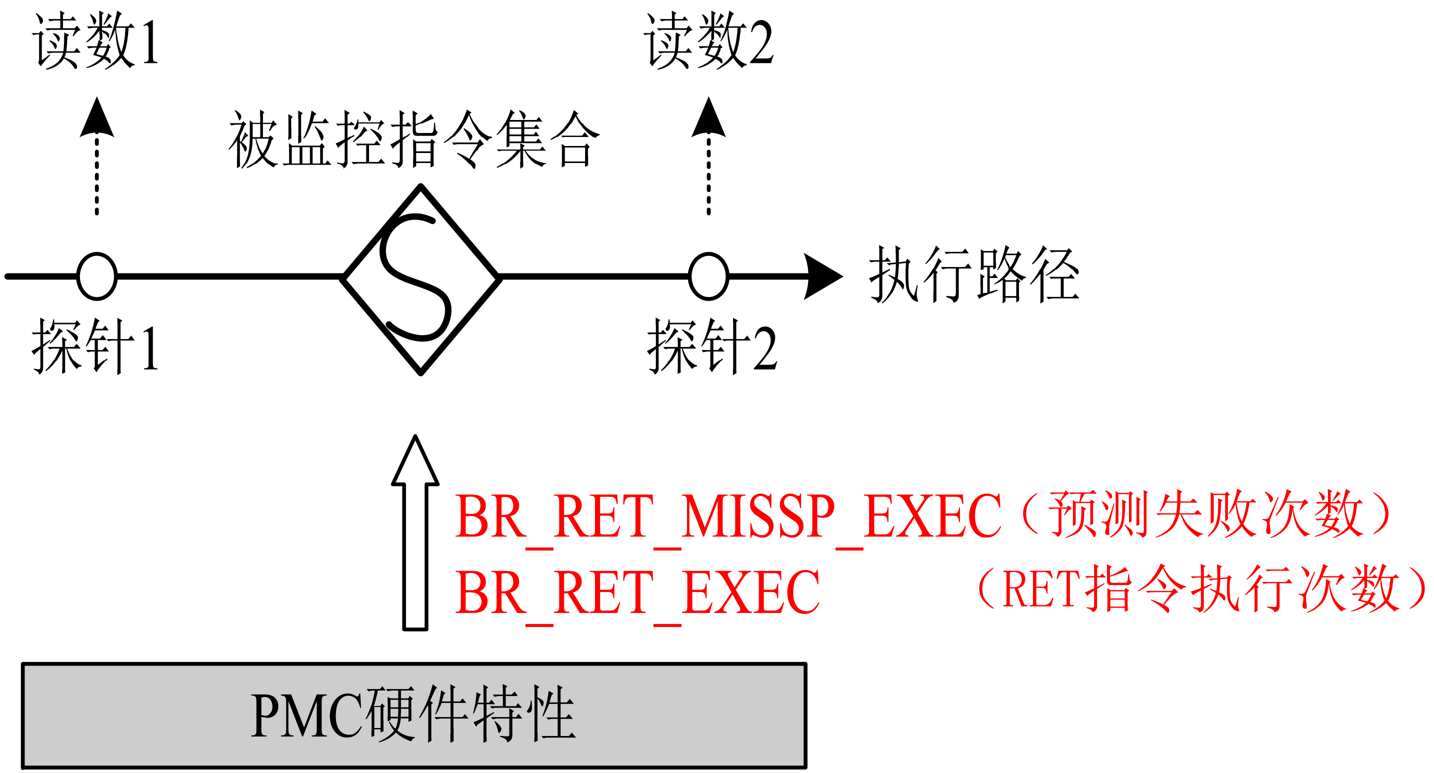
前提： 完整性基准x

```
利用PMC收集 va和vb。
if vb-va<=x then
    当前转移是合法的.
else
    if 前后探针是匹配的 then
        当前控制转移是非法的.
    else
        当前控制转移需要进一步检测.
    end if
end if
```

va： 前探针值

vb： 后探针值

可信评判4：检测隐藏控制流



H.W. Zhou, X. Wu, W.C. Shi, J.H. Yuan, B. Liang, "*HDROP: Detecting ROP Attacks Using Performance Monitoring Counters*," X. Huang and J. Zhou (Eds.): ISPEC 2014, LNCS 8434, pp. 172-186, 2014.

隐式指令与隐藏控制流

- 对变长指令的不同解释产生的结果
  - 隐式指令：未按设计意图解释的指令
  - 隐藏控制流：隐式指令产生的控制转移的集合

第一种解析的起始位置

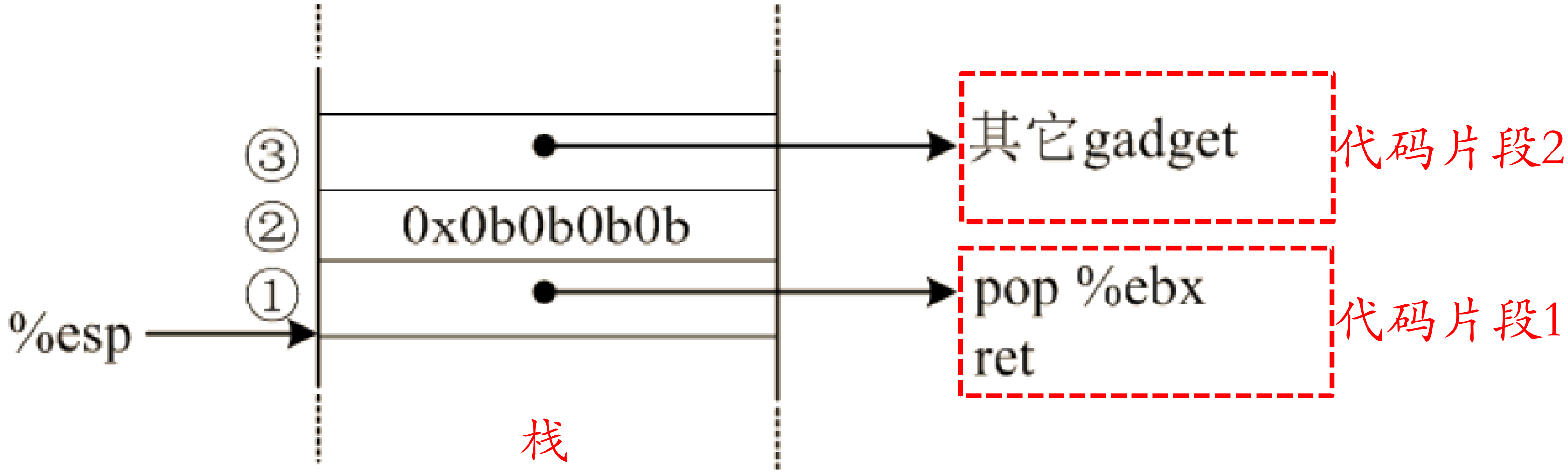
指令流：f7 c7 07 00 00 00 0f 95 45 c3

第二种解析的起始位置

第一种解析结果	f7 c7 07 00 00 00 0f 95 45 c3	test $0x00000007, %edi setnzb -61(%ebp)	解释为2条指令
第二种解析结果	c7 07 00 00 00 0f 95 45 c3	movl $0x0f000000, (%edi) xchg %ebp, %eax inc %ebp ret	解释为4条指令

隐藏控制流典型情形：ROP攻击

- Return Oriented Programming（ROP）
  - 不需要注入新的恶意代码
  - 利用现有代码中的指令片段，重新拼接和组合，改变控制流，达到恶意攻击目的



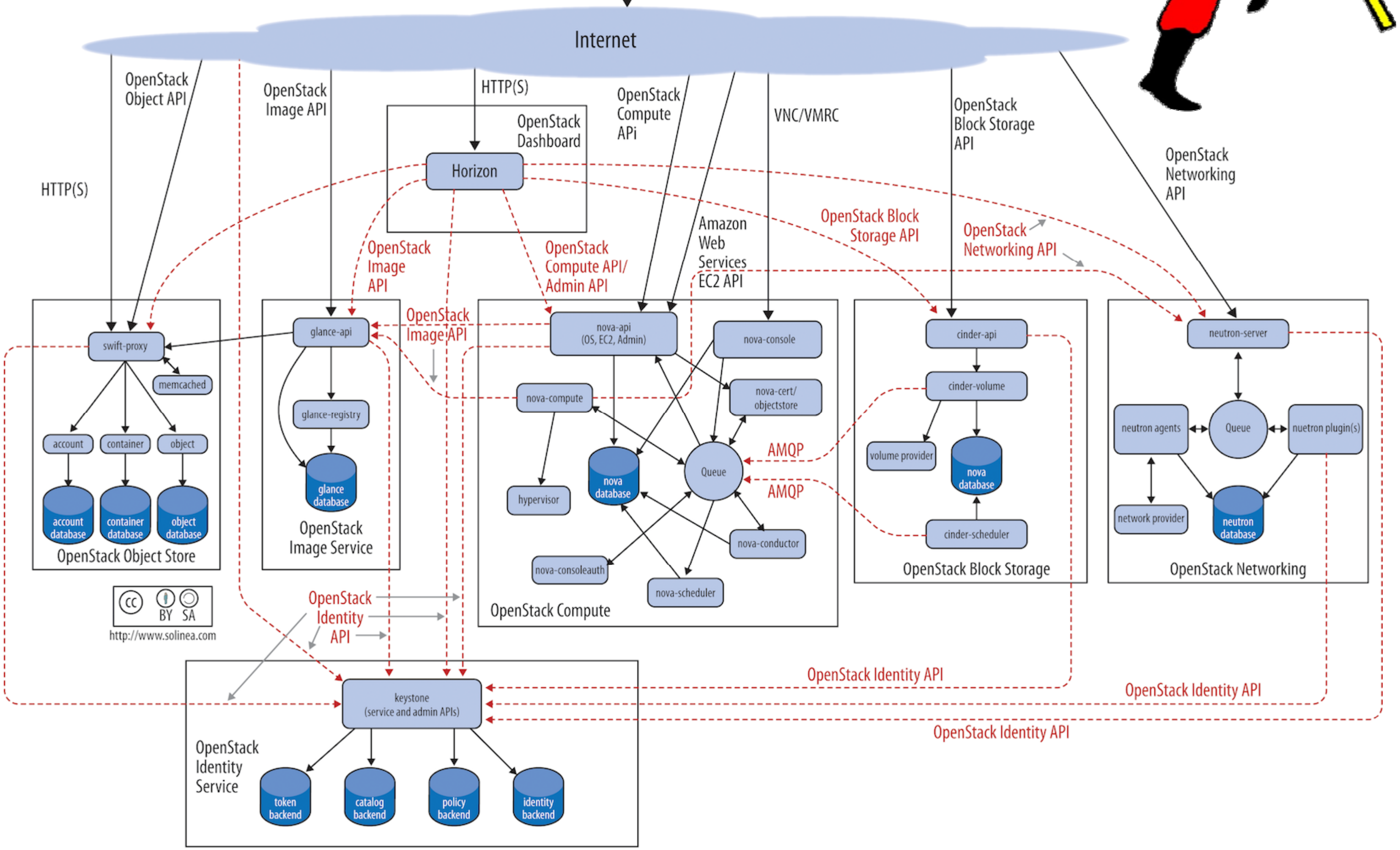
（ROP攻击示例：片段1的ret指令的执行效果就是启动片段2的执行，如此执行一系列片段。）

H. Shacham. The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86). CCS 2007.

报告大纲

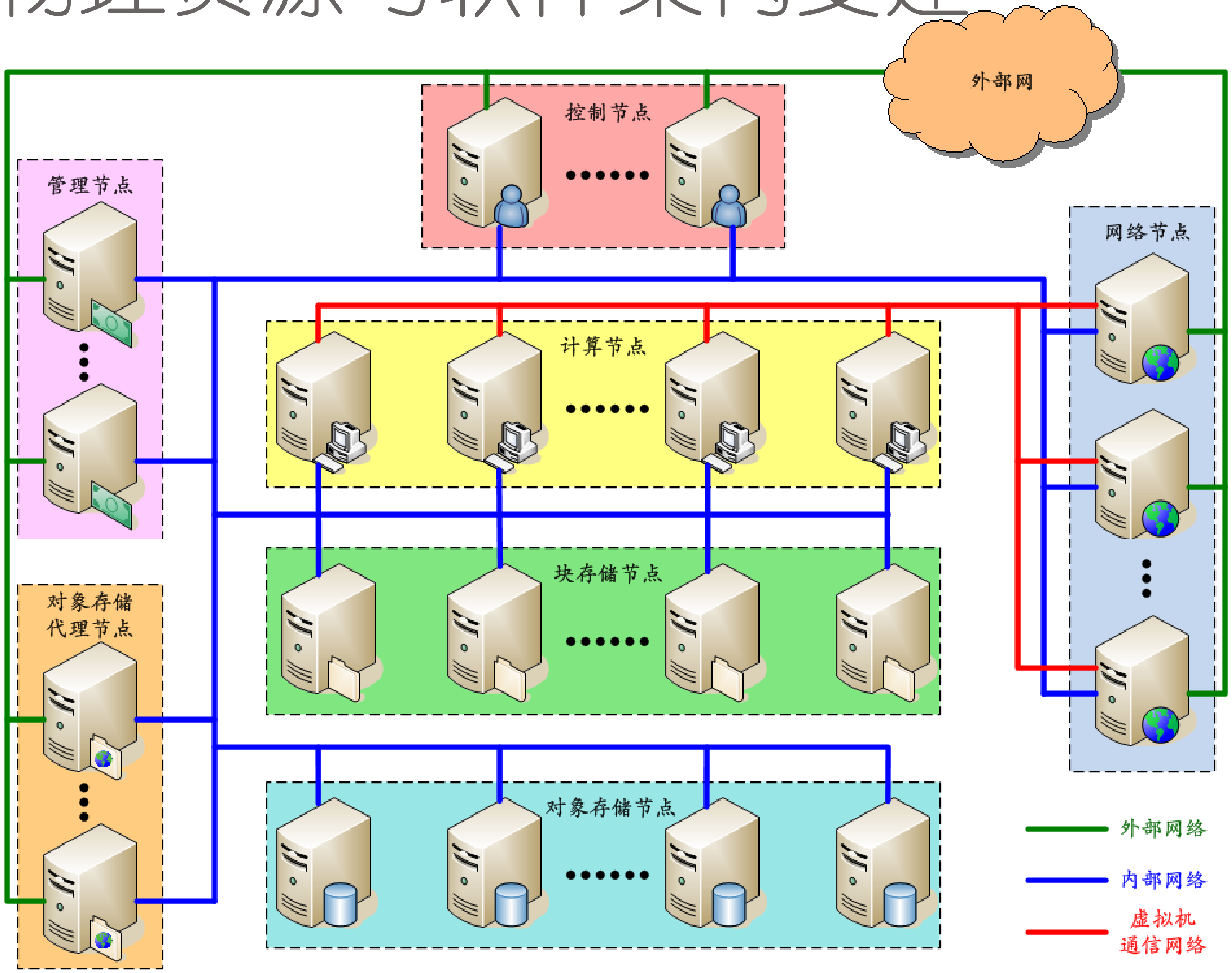
一．问题与思路
二．国际相关工作
三．已开展的工作
四．关键技术

云环境系统架构


- Command-line interfaces (nova, neutron, swift, etc)
- Cloud Management Tools (Rightscale, Enstratius, etc)
- GUI tools (Dashboard, Cyberduck, iPhone client, etc)
Internet
HTTP(S)
OpenStack Object API
OpenStack Image API
HTTP(S)
OpenStack Dashboard
Horizon
OpenStack Compute APi
Amazon Web Services EC2 API
VNC/VMRC
OpenStack Block Storage API
OpenStack Networking API
OpenStack Image API
OpenStack Compute API/ Admin API
OpenStack Block Storage API
OpenStack Networking API
OpenStack Image API
swift-proxy
memcached
account
container
object
account database
container database
object database
OpenStack Object Store
glance-api
glance-registry
glance database
OpenStack Image Service
nova-api (OS, EC2, Admin)
nova-console
nova-cert/ objectstore
nova-compute
hypervisor
nova database
Queue
nova-conductor
nova-consoleauth
nova-scheduler
OpenStack Compute
AMQP
AMQP
cinder-api
cinder-volume
volume provider
nova database
cinder-scheduler
OpenStack Block Storage
neutron-server
neutron agents
Queue
nuetron plugin(s)
network provider
neutron database
OpenStack Networking
BY SA
http://www.solinea.com
OpenStack Identity API
keystone (service and admin APIs)
OpenStack Identity Service
token backend
catalog backend
policy backend
identity backend
OpenStack Identity API
OpenStack Identity API
OpenStack Identity API

物理资源与软件架构变迁

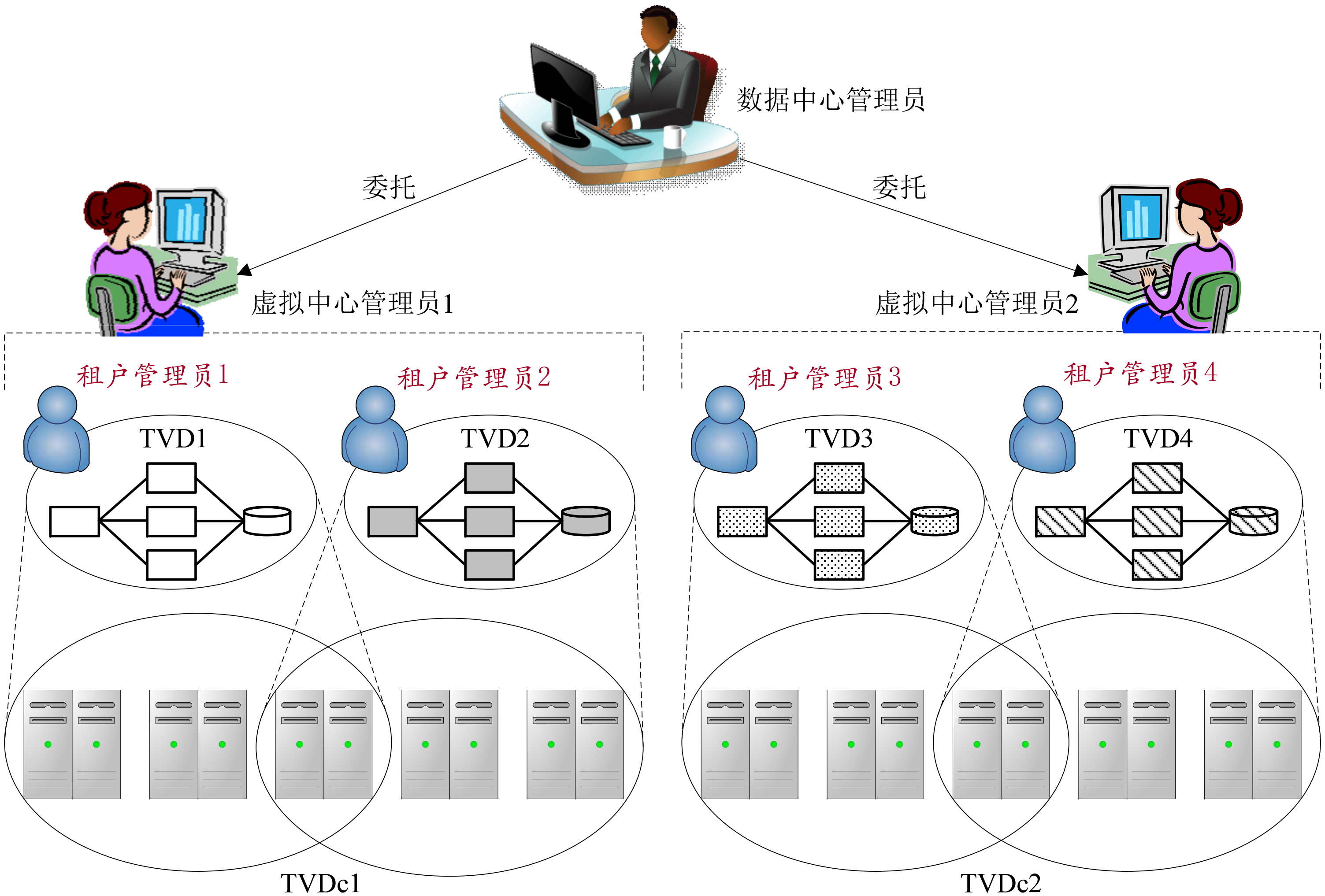
软件定义XX



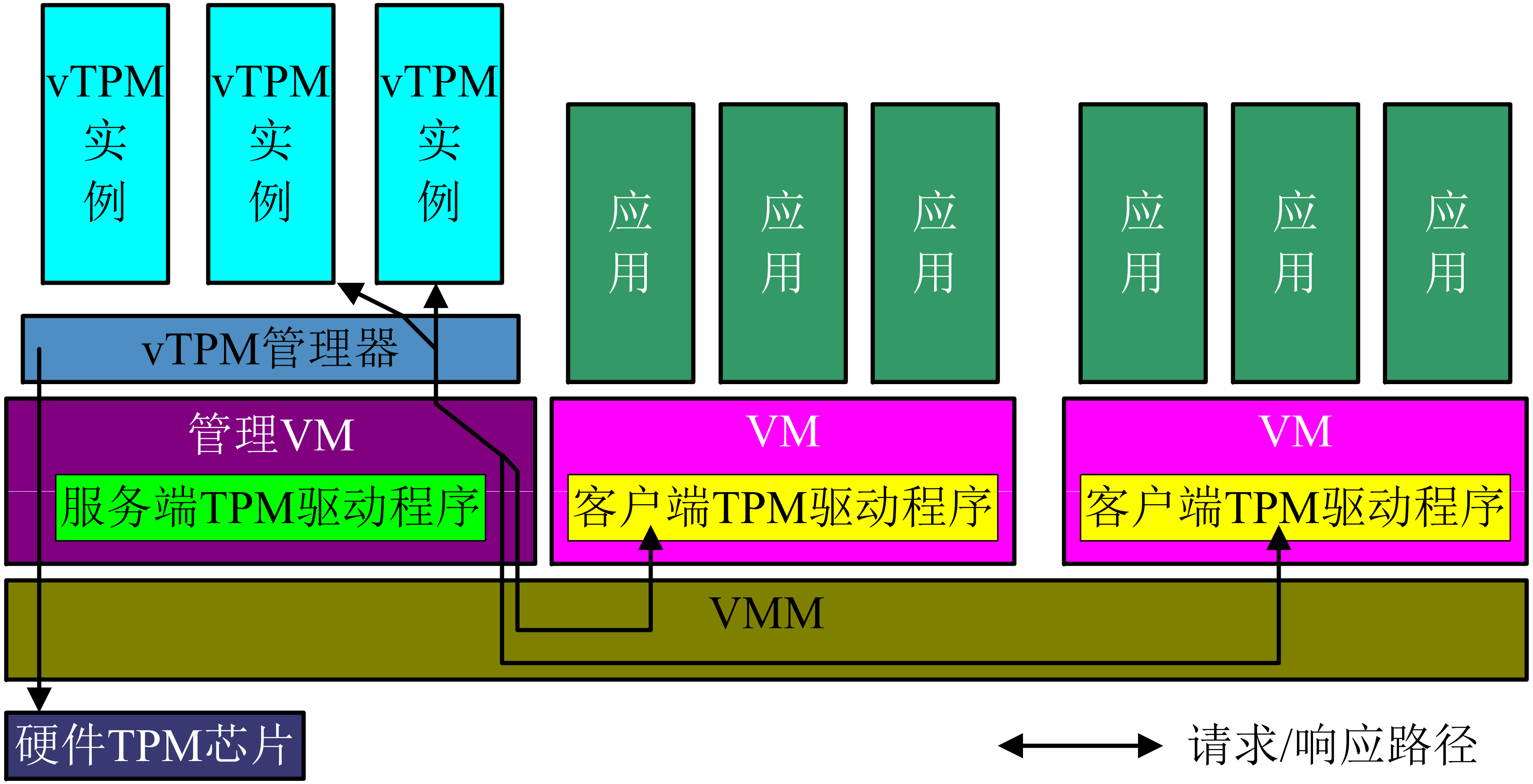
资源格局剧变

IBM沃森研究中心
IBM

可信虚拟数据中心TVDc

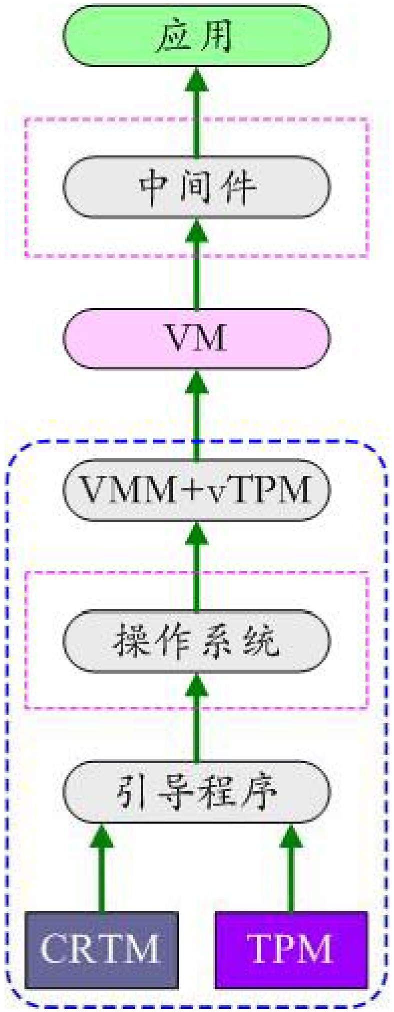


为虚拟机提供虚拟的TPM

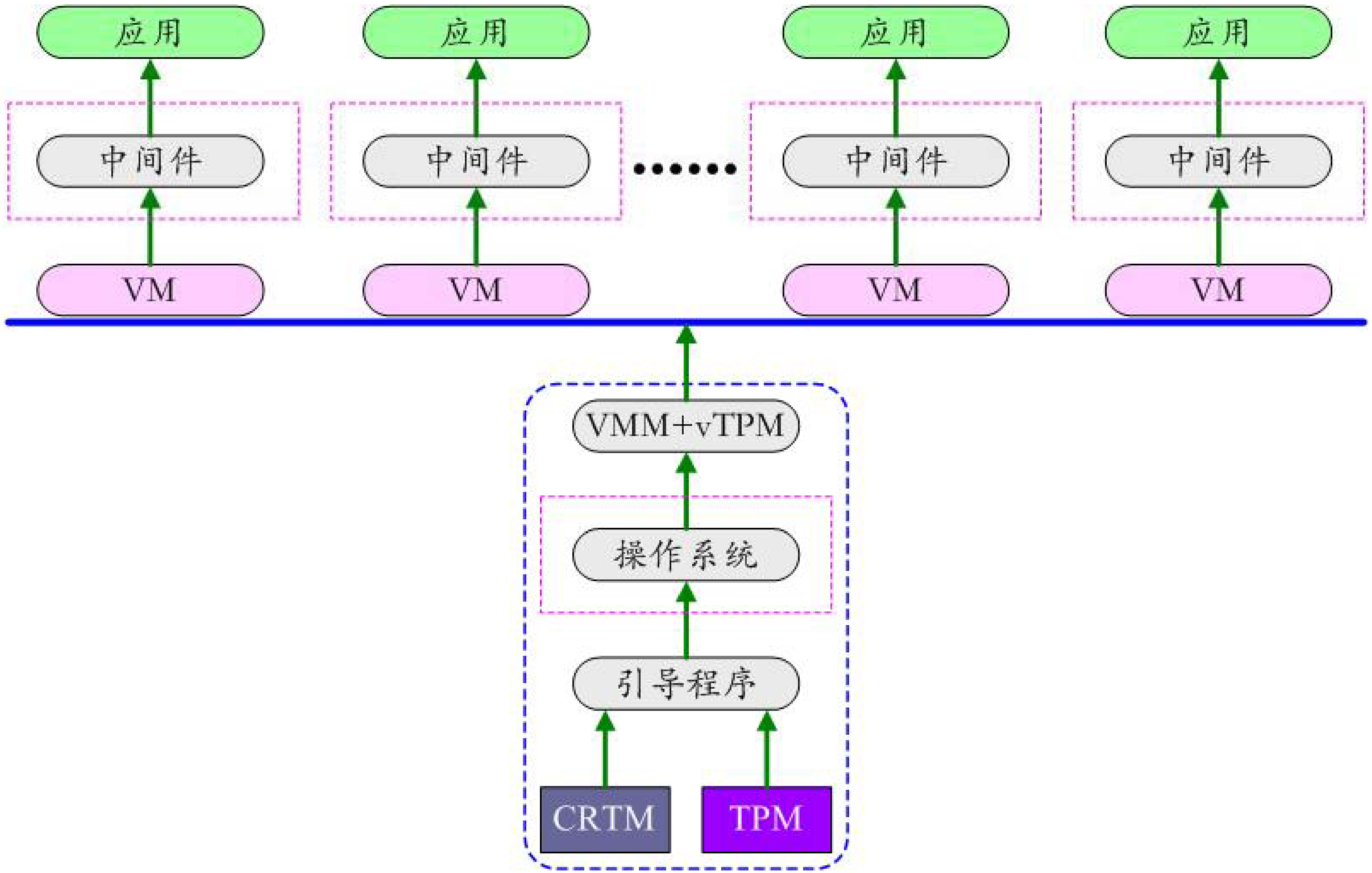


S. Berger, R. C´aceres, K. A. Goldman, R. Perez, R. Sailer, L. van Doorn. vTPM: Virtualizing the Trusted Platform Module, 15th USENIX Security Symposium (Security ’06), 2006.

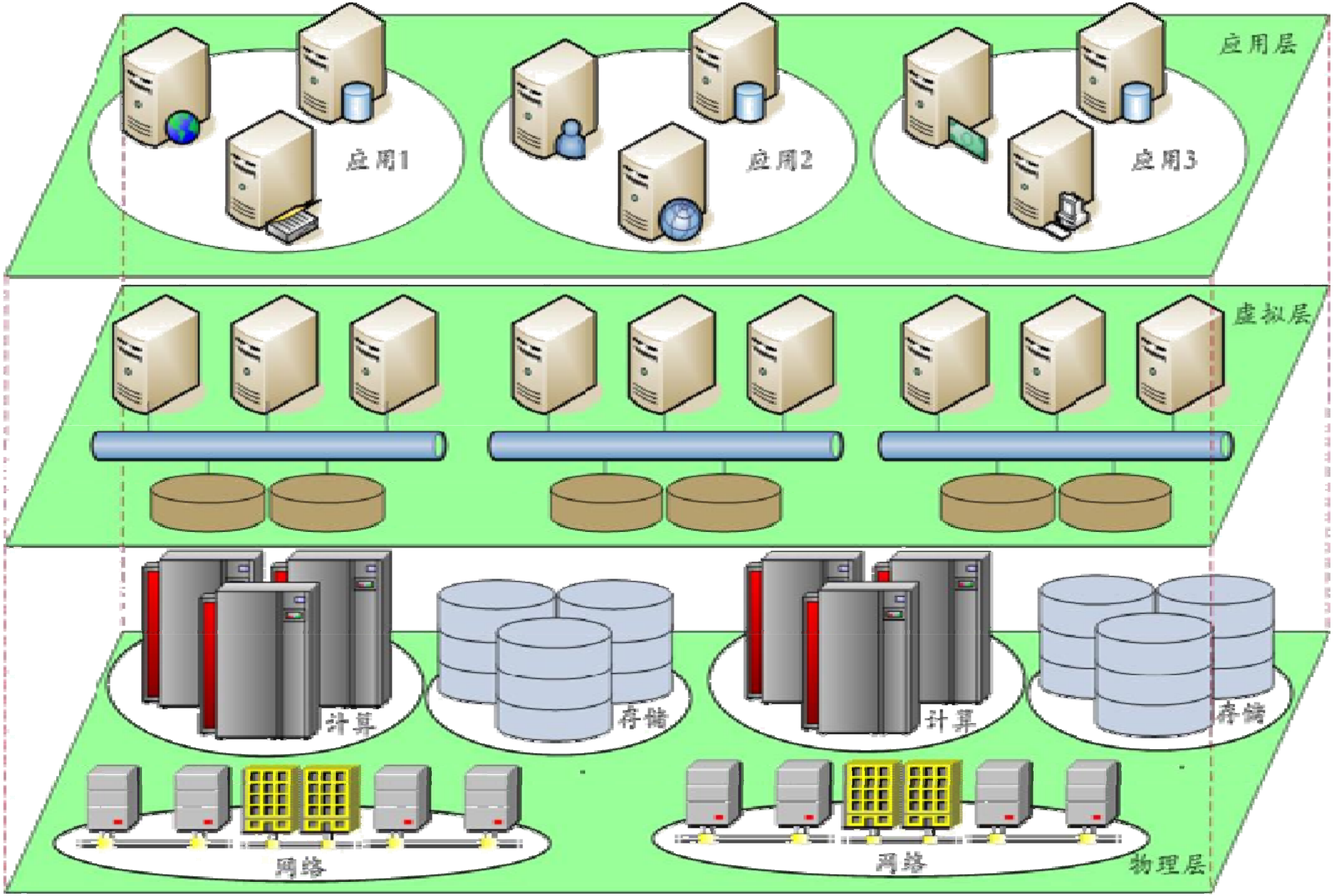
已有探测支撑架构的基本形式



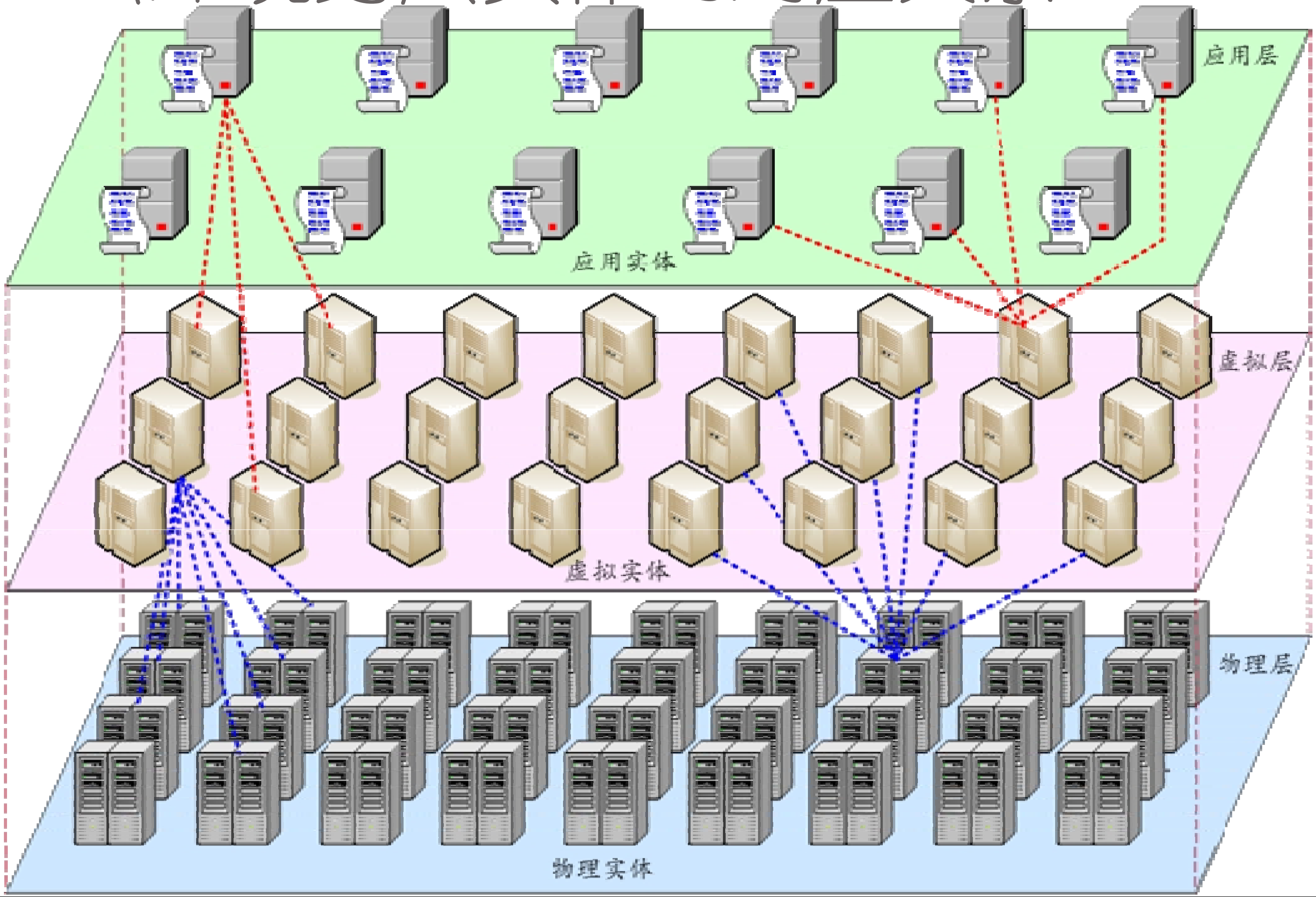
已有探测支撑架构的一般形式



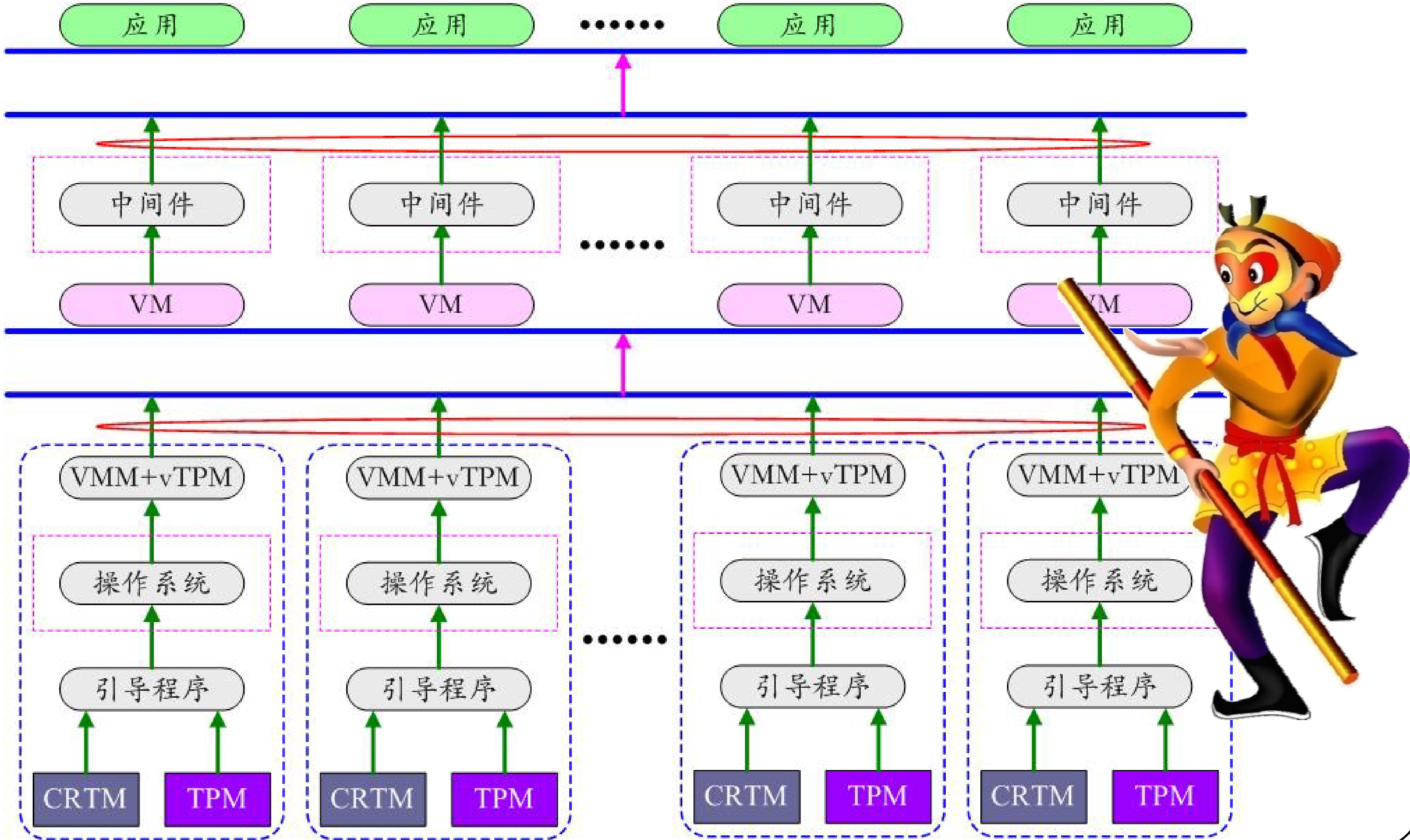
云计算的抽象层次



云环境跨层实体的对应关系



建立云端复合探测支撑体系



谢谢！