EDA Information Security and Cloud Computing

Naresh K. Sehgal[1], Sohum Sohoni[2], Ying Xiong[2], David Fritz[2], Wira Mulia[2], and John M. Acken[2]

1 Intel Corporation,
2 Oklahoma State Univ.

Contents

- Background and Problem Statement
- Cloud Computing Trends
- Information Security Background
  - Internet Security Issues
- Security Issues with Cloud Computing
  - Scenarios
  - Challenges related to Virtualization
- Future Needs

Background

- Cloud Computing (CC) refers to
  - Providing IT Services, Applications and Data
  - Using dynamically scalable pool(s),
  - Remotely residing Resources
- CC provides financial benefits to users and providers
- CC amplifies Information security issues

Are we there yet?

EDA not yet ready for cloud computing

Rick Merritt

2/2/2011 9:32 PM EST

SANTA CLARA, Calif. – Big EDA companies have their eyes on cloud computing, but their feet are still on the ground, according to a panel discussion at DesignCon here.

DAC Panel: A Reality Check On Cloud Computing For EDA

By Richard Goering on June 23, 2010

Comments(2)

Filed under: Industry Insights, DAC, SaaS, Hosted Design Solutions, Xuropa, Amazon, cloud, Kuehlmann, cloud computing, Griffith

Does IC design have a future "in the clouds?" Yes, according to panelists at last week's Design Automation Conference - but selectively, over a period of time. As attractive as cloud computing is, there are still technology challenges and tradeoffs, and the EDA licensing model for cloud computing has yet to be resolved.

What do you think is the future of EDA in Clouds?

HPC in the Cloud >> Around the Web

February 03, 2011

Cloud Still Lofty Concept for EDA Execs

Nicole Hemsoth

Problem Statements

- Access Control
  - Who can rightfully access a computer system
    - CC shares the same computer between multiple users
      - May compromise the integrity of run-time programs
      - How to ensure a timely completion of jobs?
      - Who is using the EDA license installed in the Cloud?

- Secure Communications
  - Data transfer via open channels
    - Large amounts of files transferred over public nodes
    - Large Transfer time will increase customer cost

- Data Protection in Cloud
  - Design IP theft
    - Fake login or indirect access
    - Unauthorized access in a 3rd party data-center
  - Erasing footprints after the job is done, e.g., tax data on old disk drives
  - Overdoing the security so it comes in the way of cost & performance

Internet Security Levels

		Access Control	Secure communications	Data protection	Monitoring
Software	User Application	Some login, usually relies on lower levels	Usually relies on lower levels of implementation.	Encrypt or disguise data	Access logs
	Operating System (OS)	Login	In-memory transactions		Special processes as watch dogs
	Virtual Machine Layer (VM)				
	Hypervisor Layer				
	software drivers	from OS	Encryption, security handshake	encrypt data	
	BIOS/FW based system management layer	Privileged execution		Privileged access to certain memory locations	Log files
Hardware	CPU	from OS	Port and buss encryption, secure caches	Separate secure registers and memory	
	Memory Cache / Main RAM	Encrypted busses, hash checking tables	Data encryption	Partitioning and encryption	Interrupt logs
	Memory Disk	Hash, checking tables	USB data encryption	encrypt disk storage, removable devices	Err
	I/O	Verify access id, such as internet IP address	Encrypt transmissions, trust keyboard, mouse, and audio.	Security handshake, coding, encryption	Watch dog processes in hardware and software

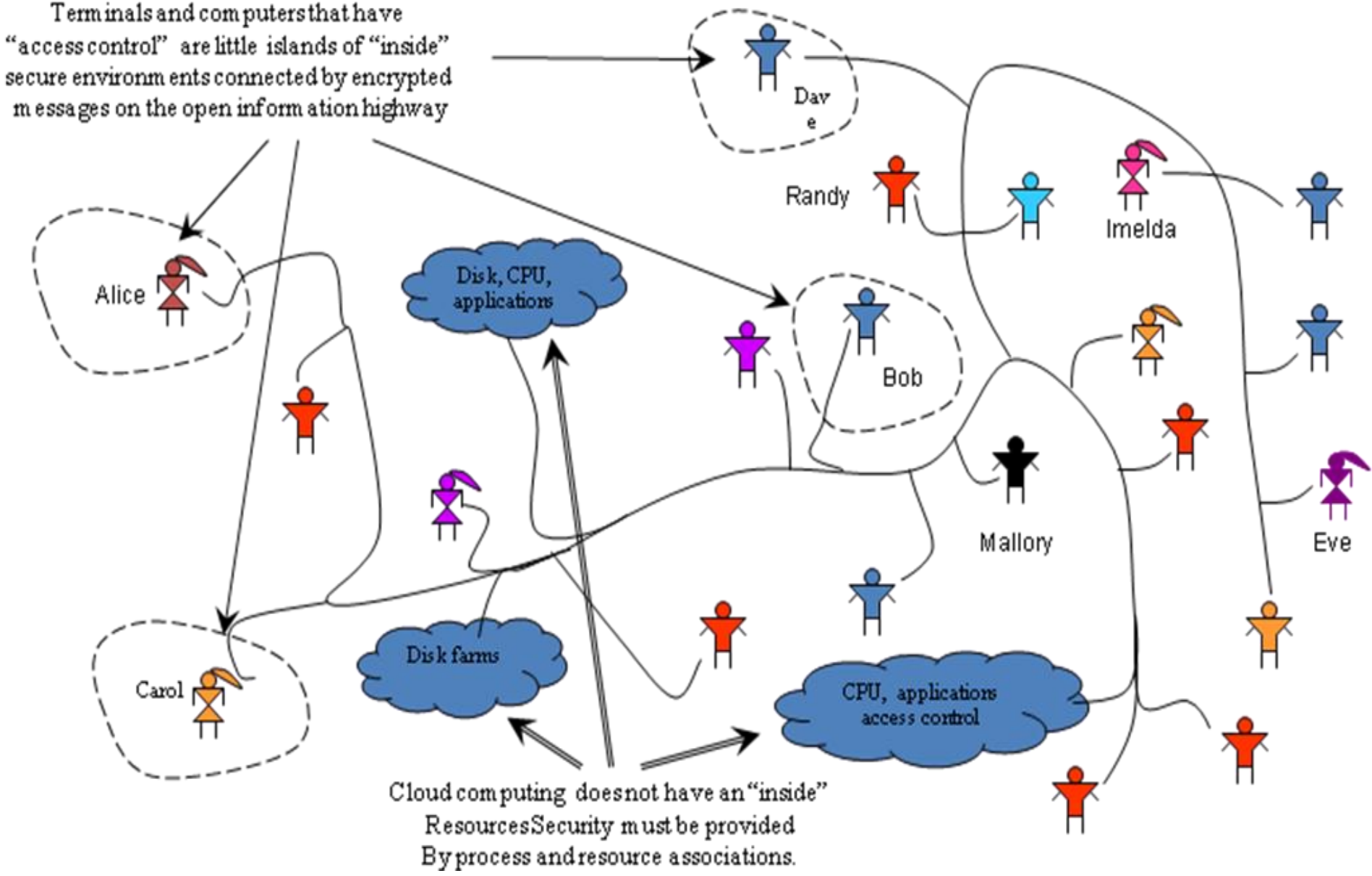
NKS

Internet Security Levels

		Access Control	Secure communications	Data protection	Monitoring
Software	User Application	Some login, usually relies on lower levels	Usually relies on lower levels of implementation.	Encrypt or disguise data	Access logs
	Operating System (OS)	Login	In-memory transactions		Special processes as watch dogs
	Virtual Machine Layer (VM)				
	Hypervisor Layer				
	software drivers	from OS	Encryption, security handshake	encrypt data	
	BIOS/FW based system management layer	Privileged execution		Privileged access to certain memory locations	Log files
Hardware	CPU	from OS	Port and buss encryption, secure caches	Separate secure registers and memory	
	Memory Cache / Main RAM	Encrypted busses, hash checking tables	Data encryption	Partitioning and encryption	Interrupt logs
	Memory Disk	Hash, checking tables	USB data encryption	encrypt disk storage, removable devices	Err
	I/O	Verify access id, such as internet IP address	Encrypt transmissions, trust keyboard, mouse, and audio.	Security handshake, coding, encryption	Watch dog processes in hardware and software

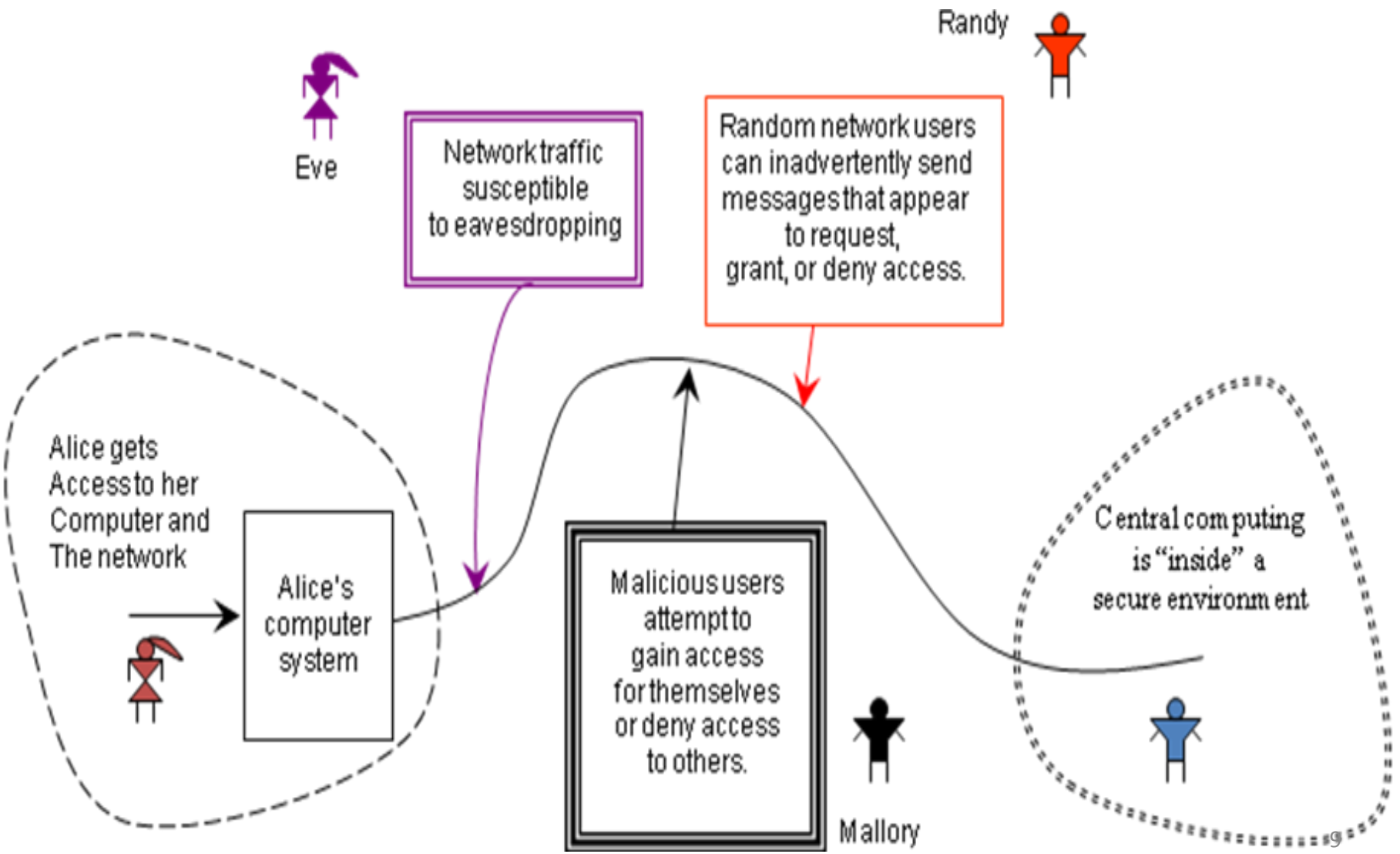
NKS

Information Security Background



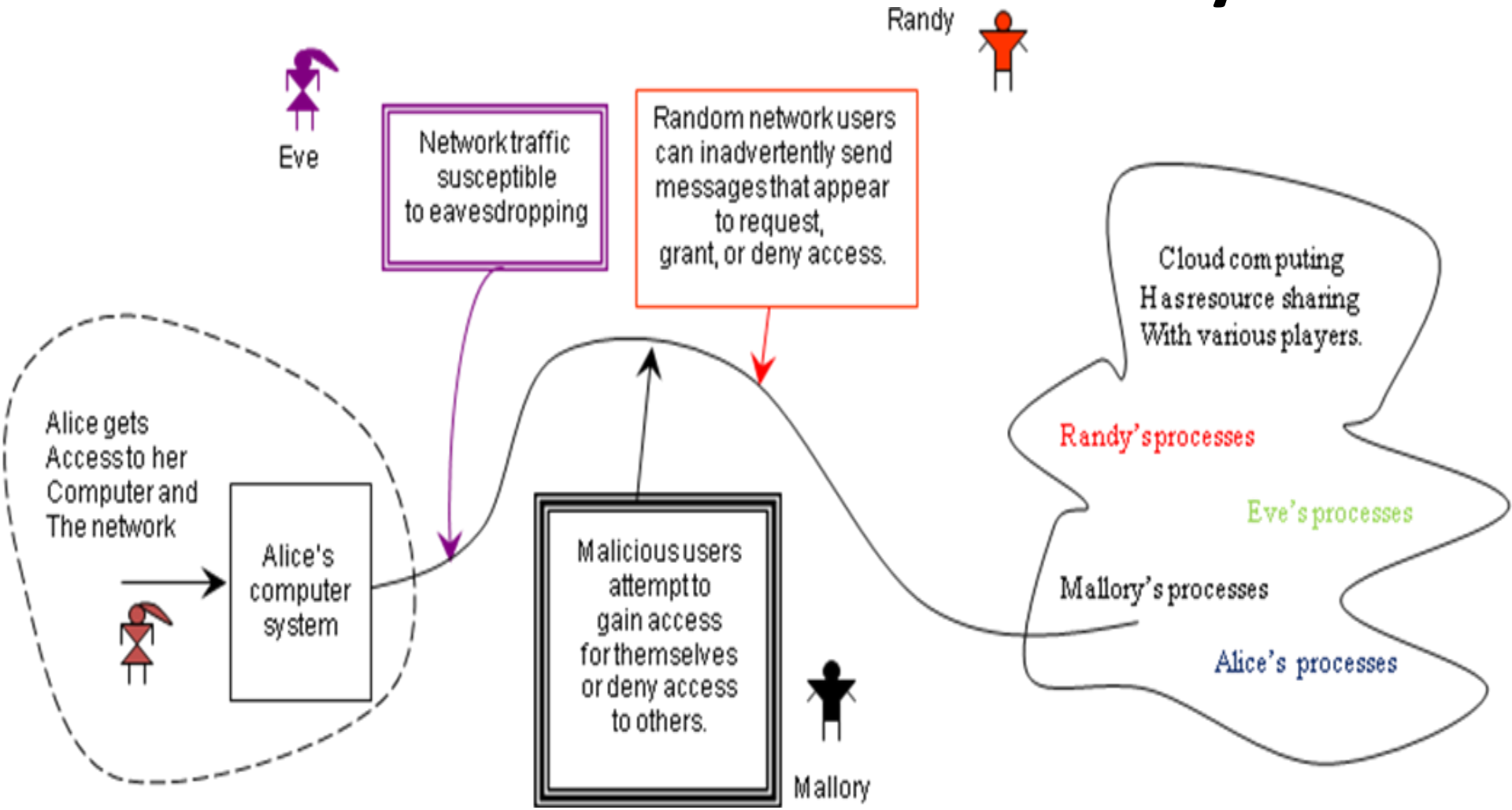
Traditional Computing Security depends upon Firewalls and Physical Security

Communication Issues between the Islands of Security



NKS

Cloud Computing Environment with No central Island of security



NKS

Security Issues with Cloud Computing

		Unauthorized data or program changes (malicious by Mallory and accidental by Randy)	Unauthorized observation and copying (intentional eavesdropping by Eve, accidental leaks to Randy)	Denial of Service attacks (intentional by Imelda and accidental by Randy)
Software	User Application	Fake login, or indirect access	Usually relies on lower levels of implementation.	
	Operating System (OS)	Fake login, low level instruction	In-memory transactions	
	Virtual Machine Layer (VM)	VM to VM communication	Information leaks	
	Hypervisor Layer			
	software drivers	from OS	encryption, security handshake	encrypt data
	BIOS/FW based system management layer	Time date stamps	Secure memory locations	Authentication for execution
Hardware	CPU	Information leaks	Information leaks	
	Memory Cache/main RAM		Information leaks	
	Memory Disk	Access privileges	Access privileges	??

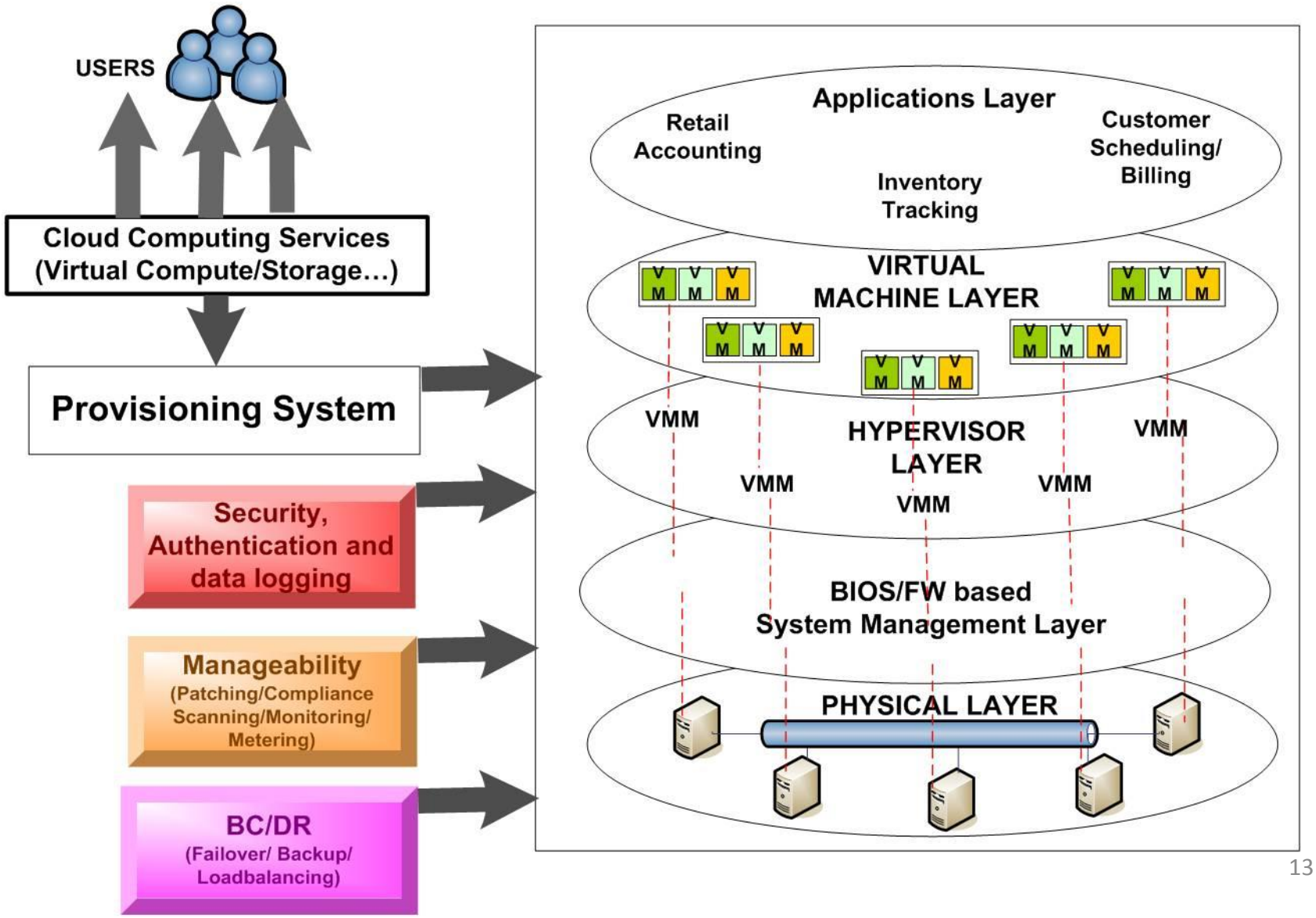
Security Issues with Cloud Computing

		Unauthorized data or program changes (malicious by Mallory and accidental by Randy)	Unauthorized observation and copying (intentional eavesdropping by Eve, accidental leaks to Randy)	Denial of Service attacks (intentional by Imelda and accidental by Randy)
Software	User Application	Fake login, or indirect access	Usually relies on lower levels of implementation.	
	Operating System (OS)	Fake login, low level instruction	In-memory transactions	
	Virtual Machine Layer (VM)	VM to VM communication	Information leaks	
	Hypervisor Layer			
	software drivers	from OS	encryption, security handshake	encrypt data
	BIOS/FW based system management layer	Time date stamps	Secure memory locations	Authentication for execution
Hardware	CPU	Information leaks	Information leaks	
	Memory Cache/main RAM		Information leaks	
	Memory Disk	Access privileges	Access privileges	??

But at what Cost?

12

Bottoms up Security inside a Cloud Data-center



NKS

Future Research on Security Gaps

1. Trust and confidentiality of consumers' data
2. Competitors sharing the same disks or servers
3. Accidental or intentional data-trashing activity that can go un-noticed
   – Regular Integrity checks
4. Cost of security vs. performance
5. Need a holistic approach for end-to-end security

Security will drive broader adoption of Cloud Computing