Education

Securing the Cloud - Using Encryption and Key Management to Solve Today's Cloud Security Challenges

Steve Pate – CTO, High Cloud Security
Tushar Tambay – Architect, High Cloud Security

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Abstract

Securing the Cloud - Using Encryption and Key Management to Solve Today's Cloud Security Challenges

- Moving to "The Cloud" is viewed as a path that most companies believe they will head down over the next several years. However, concern around security is the number one barrier to cloud adoption. Encryption and Key Management are important technologies that can help secure applications and data in the cloud. Companies considering moving to a cloud based infrastructure need to understand various aspects of encryption and key management - regulations guiding their use, the impact of key expiration and rotation on application performance and backup / restore / archiving, hardware versus software key management and retaining control of keys when applications and data are with a Cloud Service Provider. We will discuss industry best practices around encryption and key management, look at how various existing solutions fare on these considerations, and look at emerging solutions in this space.

Key Management Is Hard!

"Key management is the hardest part of cryptography and often the Achilles' heel of an otherwise secure system."

Bruce Schneier

Preface to "Applied Cryptography"

Second Edition

Agenda

- Virtualization, Cloud and how they relate
- Some basics on Virtualization and Cloud security
- Talking about encryption and key management
- What are the standards groups doing in these areas?
- Will the standards help us in the Cloud?
- What do customers want in terms of encryption and key management?
- Are there models in place that allow customers and providers to work together?
- It looks a little scary - is there hope?
- Where can I get more information?

The Cloud Depends On Virtualization

- Basic Costs … multi-tenancy
  - Example – websites hosted by Media Temple are VMs
- How many VMs can I run on a single server?
  - 10 or so on older servers, 25 on newer servers
  - Some deployments have 100s of VMs / host
- But really it's about flexibility
  - Heavily virtualized companies have great flexibility in their virtualized environments but can't get that flexibility in the public Cloud
- VM mobility is key
  - VM and data need to stay together
  - Customers need control over VMs in public clouds
- Cloud bursting - just all talk?
  - The dynamic deployment of a VM that runs on internal organizational compute resources to a public cloud to address a spike in demand.
  - How do I move that much data in and out of the cloud dynamically?

Virtualization Has New Challenges

- Many different areas – we're focusing on data security
- The idea of machine theft becomes a reality ➠ USB key ...
- My memory image is now in a file (paging, snapshots, suspending, ...). Protection in the guest has new issues
- Some problems existed in the physical world – VMs are more easily exploited
  - Encryption keys used in memory can be found in files on disk!
  - Running AD as a VM? Lots of usernames/password on disk in the clear
- VMs needs to be wrapped when moving in and out of the cloud – SSL/TLS not enough

"Have all defense in depth mechanisms work together. Security needs to follow VMs in the infrastructure."

VMware CEO Maritz - VMworld 2010

And So Does The Cloud …

- Many areas of concern - the main issue is around data and protecting the data!
- I sign up for on-line services - taxes, Wiki, ...
  - On-line Wikis – ACLs don't prevent admins from reading data
  - New security startup - wants to use cloud services, concerned about putting source code in the cloud, wants easy to use tools, …
- My data gets backed up but ..... where does it go?
  - Disk-to-disk, to tape, this country, somewhere else, …?
- Move from CSP to another:
  - How can they delete the data?
  - Can they find all of those tapes?
  - For data backed up on tape, can one customer's data be shredded?

And So Does The Cloud … cont

- Is Multi-Tenancy really a problem?
  - VM guest to guest attacks
  - A VM takes over the hypervisor - how real is this?
  - We separate data either through logical or physical means
    - Does this really help? Isn't it all still on disk side by side?
- It's all about people
  - We can put best security tools and best practices in place but …
  - … in a recent survey:
    - 33 percent of IT professionals were most concerned about data being lost or stolen through USB devices.
    - 39 percent of IT professionals worldwide were more concerned about the threat from their own employees than the threat from outside hackers.
    - 27 percent of IT professionals admitted that they did not know the trends of data loss incidents over the past few years.

So where do we stand?

- *Only 34% of Servers are virtualized .... the #1 restriction sited to further virtualization was security* – CDW 2009
- *87% of respondents rated "Security Challenges" as the #1 issue ascribed to the Cloud model.* – IDC Enterprise Panel 2009
- *"73 percent said security was the primary obstacle to their adopting cloud computing, followed by compliance (54 percent) and portability and ownership of data (48 percent). Most said they were worried about stopping unauthorized access to their company data in the cloud, and 42 percent said security worries have stopped their organizations from going to the cloud."* – PhoneFactor survey

- *"By 2015, security will shift from being the No. 1 inhibitor of cloud to one of the top enablers"* – Forrester Research

How Can Encryption Help?

- Industry leaders and organizations recognize that encryption is a critical component of secure cloud environments
- The key to this is key management
  - Encryption will not be widely deployed unless it is easy to use
  - Think back to the Bruce Shneier quote
- Leading think tanks are putting together new guidelines
  - But technology is lagging …
- Industry wide initiatives needed to address:
  - Standards
  - Best practices
  - The human factor
  - How technology fits into the new world

But Isn't Encryption Slow?

- How much hardware to throw at the problem:
  - Similar to the multi-tenant cloud analogy
  - How much memory do I have?
  - Am I CPU bound or I/O bound?
- Multiple hardware options available
  - Instructions built into the CPU – libraries available in public domain
  - Numerous hardware cards available
  - Many cards offer more than just encryption (key generation and storage, tamper proof capabilities)
- Will see some hardware options become commonplace over next several years

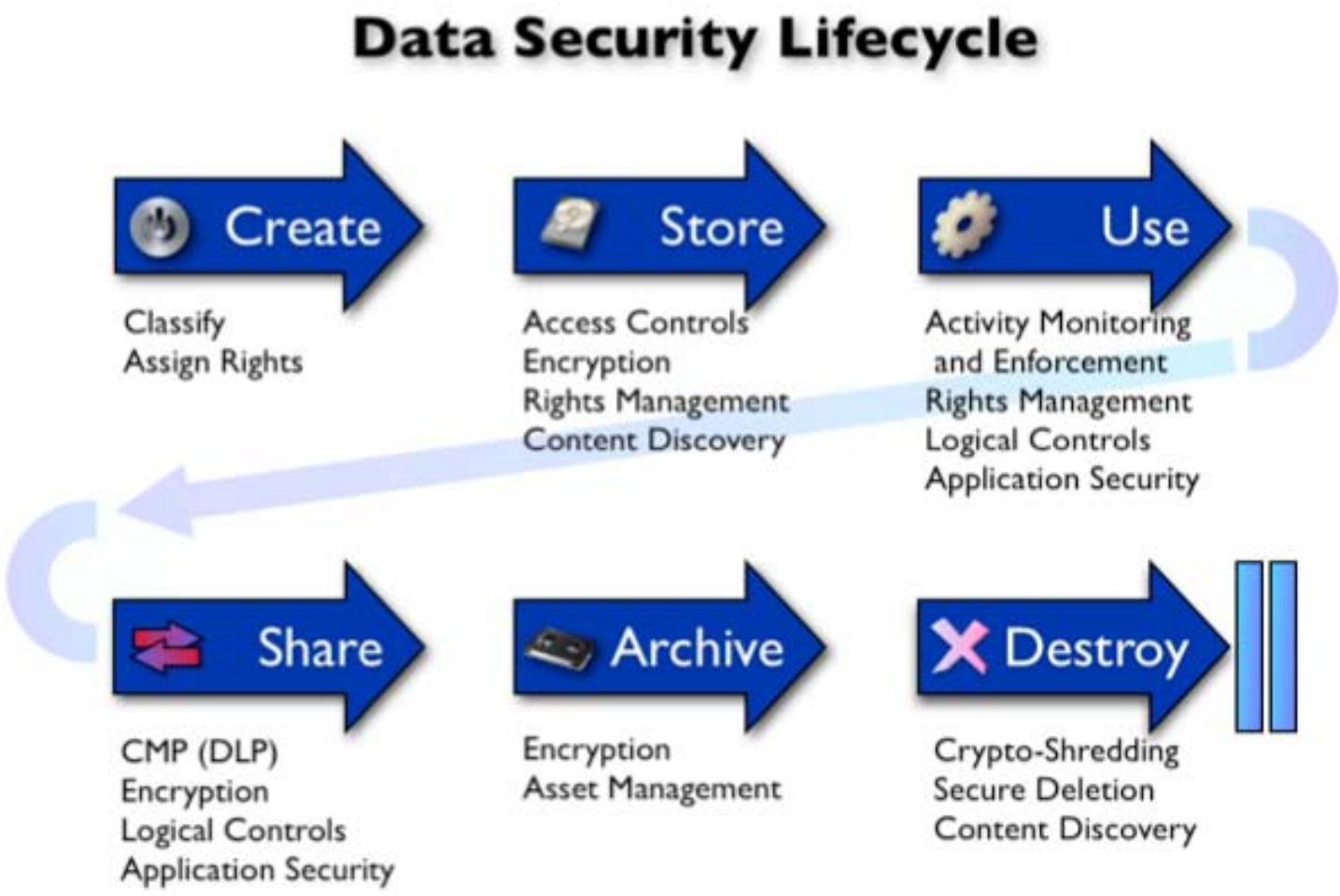
Industry Forums / Leaders?

- Standards are still in their infancy
- CSA – Cloud Security Alliance
  - A non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.
- ENISA – European Network and Information Security Agency
  - ENISA is the EU's response to security issues of the European Union. As such, it is the 'pace-setter' for Information Security in Europe.
- Jericho Forum – part of the Open Group
  - The leading international IT security thought-leadership association dedicated to advancing secure business in a global open-network environment.
- NIST, OASIS, SNIA, Open Group, OCC, DMTF, …

Some Guidelines Available

- CSA – Cloud Security Alliance:
  - *Top Threats to Cloud Computing V1.0* – March 2010 (14 pages)
  - *Security Guidance for Critical Areas of Focus in Cloud Computing Prepared by the Cloud Security Alliance* - April 2009 (83 pages)
  - *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1* – December 2009 (76 pages)
  - *CSA Cloud Controls Matrix v1.1* – December 2010 (Excel spreadsheet)
- ENISA
  - *Cloud Computing Benefits, risks and recommendations for information security* - November 09 (125 pages)

What About The Data?



Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 – CSA - December 2009

Encryption and Key Management

Check out these SNIA Tutorials:

Cryptography Deciphered – Michael Willett, Spring 2011

An Inside Look at Imminent Key Management Standards - Matthew Ball, Spring 2010

An Introduction to Key Management for Secure Storage – Walt Hubis – Spring 2010

Visit the Cloud Storage Hands-On Lab:

Encryption and Key Management

- What do the standards recommend?
  - NIST (National Institute of Standards and Technology) provides recommendations on algorithms and encryption modes
  - Need to be aware of FIPS (Federal Information Processing Standards) certification, Common Criteria and similar standards in other countries
- Is this enough in a distributed cloud-based world?
  - No – not really – different countries have different requirements
  - In some countries encryption is heavily regulated
  - Export compliance issues to be resolved
  - Need an architecture that supports multiple encryption algorithms or has a pluggable architecture that allows for new algorithms
  - Key management standards are not sufficient.

Encryption / Key Management Issues

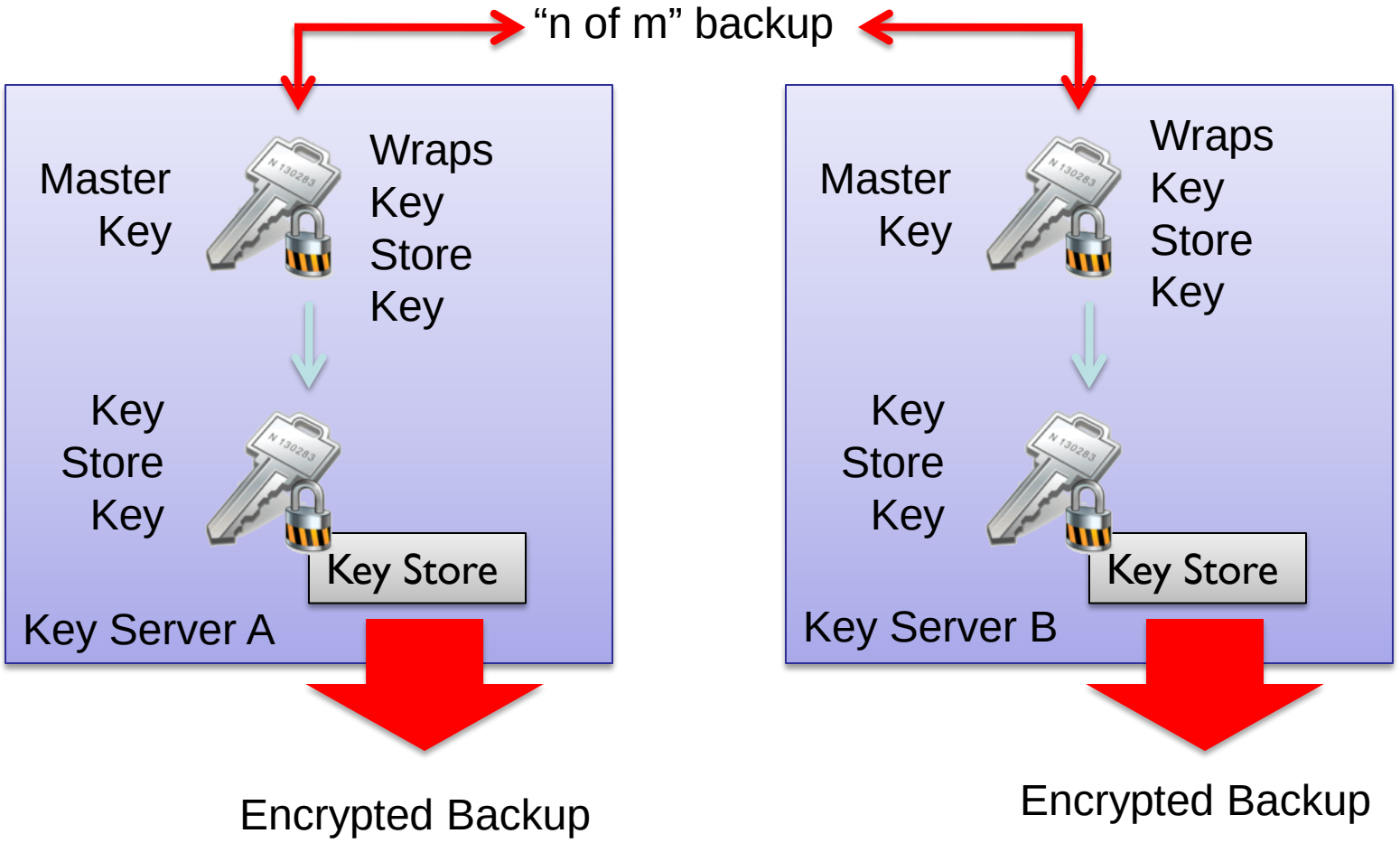
- Key generation and key application - Two different areas – often confused
  - Key Management
  - Application of keys at the endpoint
- Administrative roles
  - No good if one person has access to everything
- Key Lifecycle
  - Key states:
    - Pre-activation, Active, Suspended, Revoked, Deactivated, Destroyed, Compromised, Destroyed Compromised
  - Key state transitions
  - Roles and responsibilities
  - Key meta data, storage, transport, escrow, backup, recovery, revocation, suspension, renewal, compromise, …

A Framework for Designing Cryptographic Key Management Systems – NIST special publication 800-130 (84 pages)

Key Management Issues

- What do we care about?
  - Key generation and key application
  - Protection of the keys - Key encryption / Master key
  - How to protect the master key
  - High availability and disaster recovery scenarios
  - Key expiration / rotation – what happens to the data?
  - Key shredding / switching to other states (read only)
- There is poor integration between key management systems, the application of encryption and the data lifecycle
  - This is why many of today's key management techniques don't work
- Many encryption "solutions" tend to be home grown
- Key management should be hidden within a policy framework

Key Management Server Example

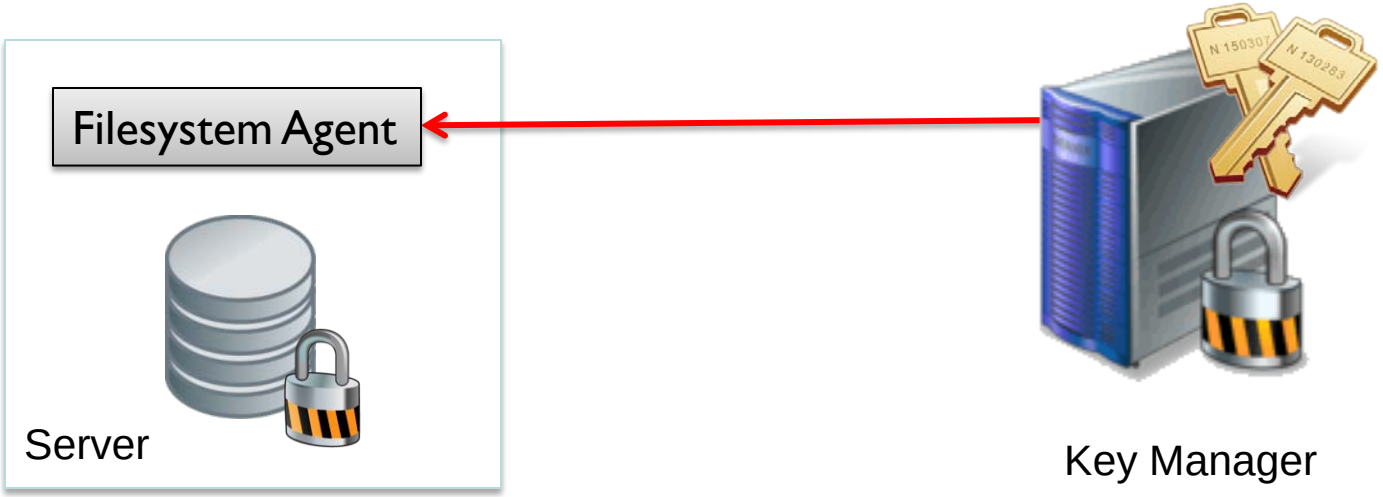


Key Management Standards

- IEEE 1619.3
  - Disbanded in Dec 2010
- OASIS KMIP
  - Publicly announced in February 2009
  - KMIP V1.0 was approved in September 2010
  - http://docs.oasis-open.org/kmip/spec/v1.0/os/kmip-spec-1.0-os.pdf (152 pages)
  - Looks like companies are moving ahead to implement KMIP within their frameworks
- Other groups:
  - ISO/IEC 11770
  - ISO 11568
  - NIST SP 800-57
  - IETF Keyprov (RFC 6030, RFC 6031, RFC 6063)

Encryption At Rest – An Example

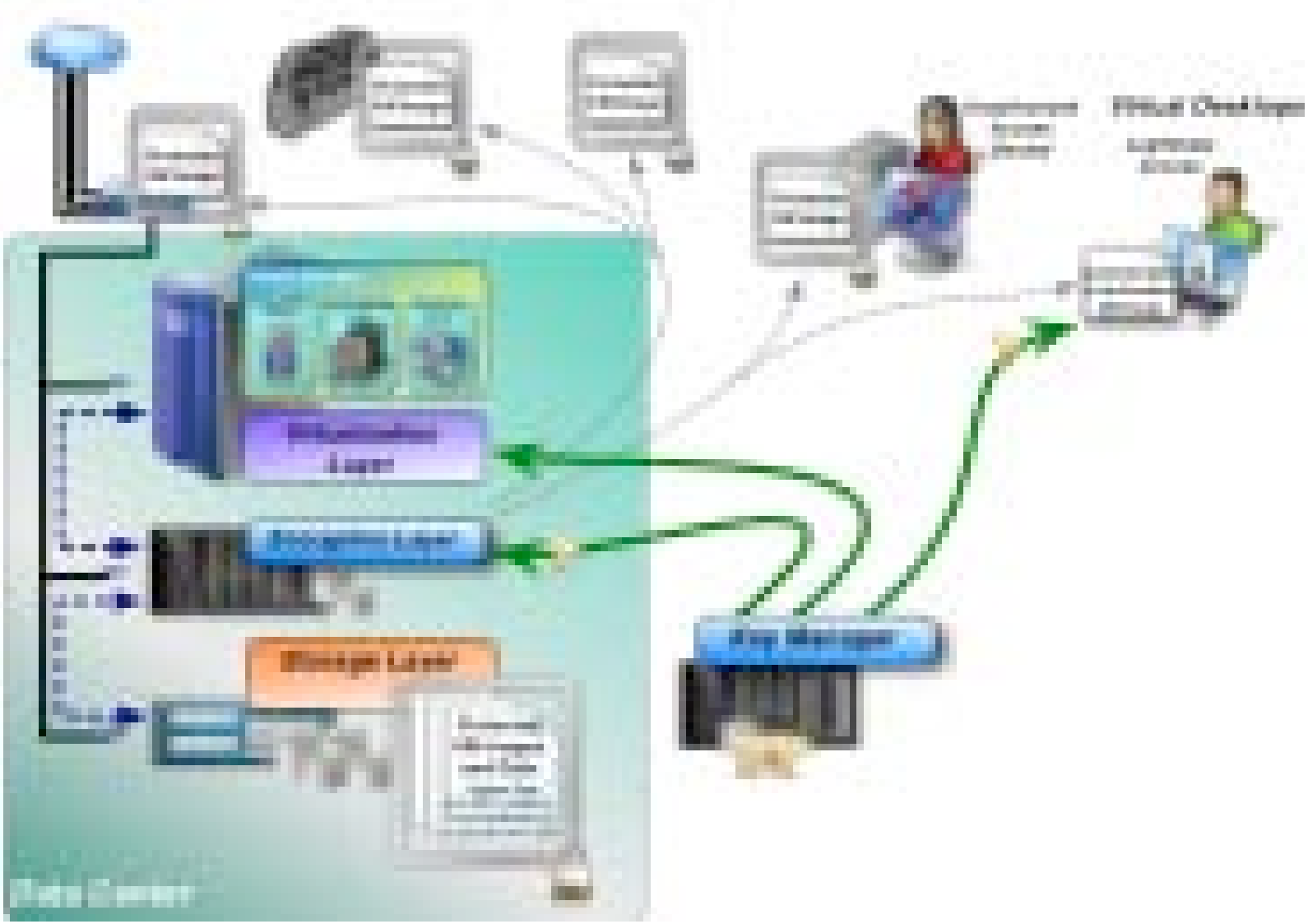
- A key is generated
- The key is securely passed to the encryption agent
  - A filesystem in this case. At this layer we have better visibility into applications, users etc and have greater access controls.
- Encryption is performed on the data
- Are we done? Not even close!



Encryption At Rest – Issues

- Does the key manager have context?
- What happens when the endpoint reboots?
  - Association of meta-data that references the key
- What happens when data is backed up?
  - Can we store meta-data with the data on backup? No so easy …
- What happens when the data is restored?
  - Can we still find the keys?
- How do we perform key rotation?
  - Does the server need to be off-line?
- In Short:
  - A great solution requires knowledge within the KM about how the keys will be used. The encryption endpoint requires integration with a number of different technologies to be effective.

Now We have Virtual Machines!



Encryption Everywhere?

- Due to VM mobility:
  - Encryption needs to be applied in multiple places
    - The encryption "endpoint" moves!
    - In the data center
    - Between data centers
    - Between private and public clouds
  - We're protecting more than just application data
  - We're dealing with new security issues
  - Where are all my VMs? I should not be concerned about this.
- Security policies need to travel with the VM
- The relationship between a key manager and the endpoint has gotten more complicated

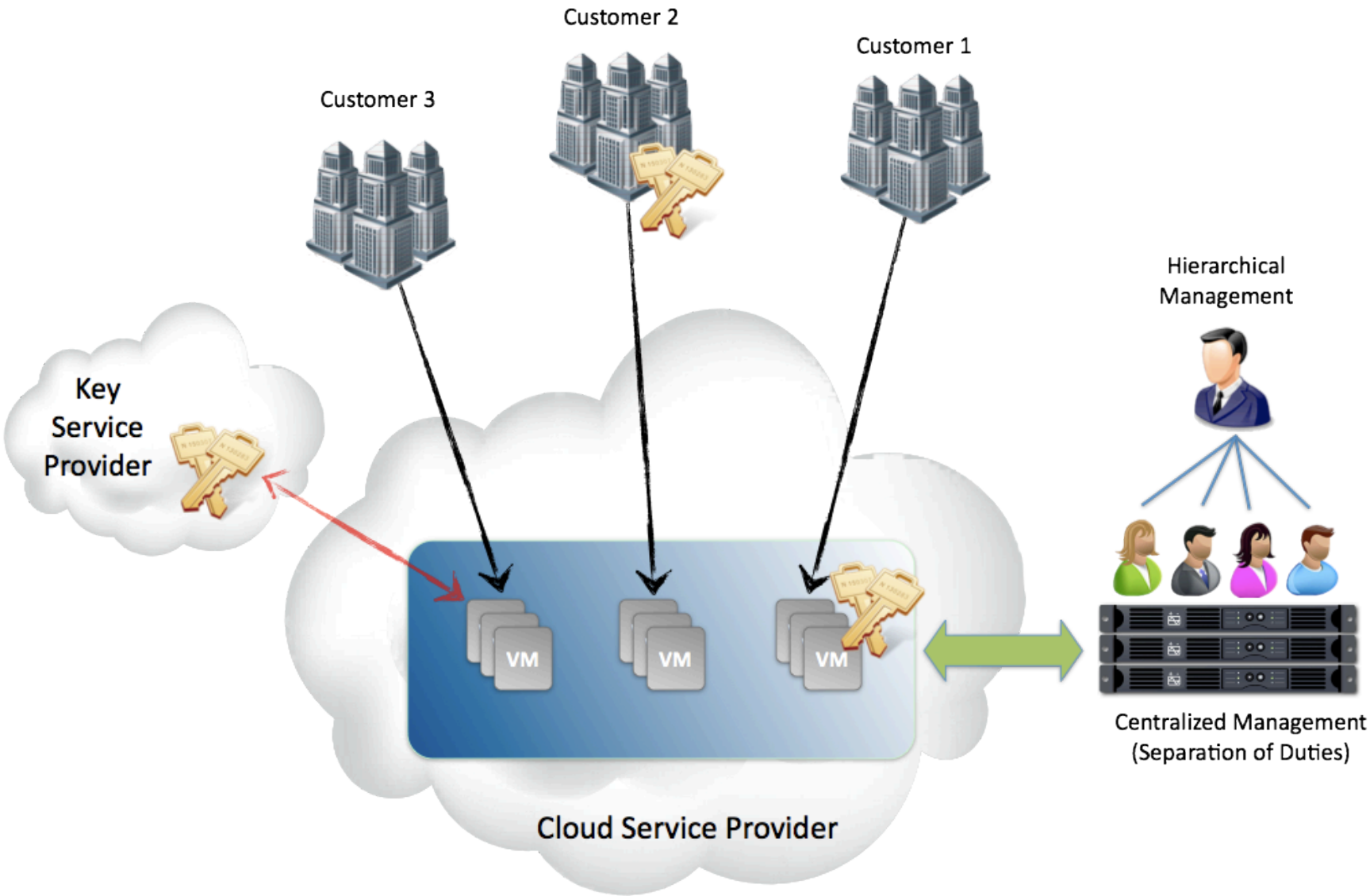
Can We Encrypt Everything?

- VM sprawl increases the amount of data
- We need deduplication to help solve the data explosion issue
  - 6.8 exabytes generated every 2 days
  - 2 years ago - $1 on virtualization, $3 on storage
  - Today - $1 on virtualization, $5 on storage
  - Some people are saying that it's more like $7
- But dedup and encryption don't always work well together
  - Need to understand dedup needs and options
  - Dedup first then encrypt?
  - Interesting multi-tenancy issues
- Storage in the virtual world is not the same as the physical
  - We need to think different about how we manage this imbalance
  - Especially considering everything moves as a container

Stop Thinking In Terms Of Keys!

- Key Management should be hidden within a policy framework
- Rather than thinking:
  - Give me a key
  - Encrypt the data
  - Wrap the key in a password
  - Store the password "somewhere".
- We need to think in terms of policy:
  - I want to create some VMs and run them in my private cloud
  - My auditor wants keys rotated every 6 months
  - I now want them to move to the public cloud
  - I only want them to run Mon-Fri
  - At the end of the quarter I don't want them to run at all
  - At that point I want them gone – no trace left!

Key Management Cloud Options



Why Is It So Hard?

- The technology is so broad:
  - Operating systems
  - Storage
  - Encryption and Key Management
  - Virtualization and VM mobility
  - Cloud
- Few companies have the ability to span all
- But encryption is the solution to protect data
- Key Management solutions need to be broader
- We have the technologies today
  - We need to bring them all together

Holding The Keys To Your Kingdom

- How will the transition to public cloud work?
  - Virtualize internally – build out private cloud
  - Be confident that this environment is secure
  - Move to the public cloud as required
- Companies secure their virtualized data center
  - Build out private cloud
  - Solve key management needs for the private cloud
  - Once security needs can be met, can public clouds just be an extension?
- Service Providers secure their data centers
  - Service Provider secures their virtualized environment
  - Either CSP manages keys or customer manages keys
  - Different companies will have different requirements / needs

For More Information

- ENISA
  - http://www.enisa.europa.eu/
- Cloud Security Alliance
  - http://www.cloudsecurityalliance.org/
- NIST
  - http://www.nist.gov
- Encryption / Key Management Links
  - http://xml.coverpages.org/keyManagement.html
- OASIS KMIP
  - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip
- Virtualization Practice – great podcast
  - http://www.virtualizationpractice.com
- Trend Micro Cloud Blog
  - http://cloudsecurity.trendmicro.com
- SNIA Resources (search for "encryption" and "key management")
  - http://www.snia.org/home

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

- SNIA Education Committee

Steve Pate
Tushar Tambay