Cybersecurity Fundamentals

BITSYM LABS

Contents

Cloud computing

- Definition
- Cloud computing services
- Cloud security
- Backups and Cloud computing

BITSYM LABS

Next

Definition of Cloud Computing

BITSYM LABS

Cloud Computing

What is a cloud?

cloud com·put·ing

noun

the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

- The "remote servers" are virtual computers on data center hardware
  - You can do virtualization without doing cloud
  - You cannot do cloud without using virtual computers

Software as a Service (Saas)

- Cloud provider supplies and manages:
  - Hardware, OS, software, and data storage
  - Gmail, Google Apps, Salesforce, GoToMeeting
- Customer accesses the software app via the internet:
  - Most commonly via a browser (can be a provider supplied application)
  - An example of a thin-client model
- The customer has little control over any part of the experience:
  - But then, the customer does not have to worry about any of that either
  - The only IT expense for the customer is desktop (or laptop or tablet) that can run a browser

Platform as a Service (PaaS)

- Cloud provider supplies and manages:
  - Hardware, OS, core system applications
  - Also provides the data storage
  - Responsibilities:
    - Sets up the virtual server and grants the customer the access
    - Keeping the system running and keeping OS patches in place

- Customer provides and manages:
  - Production applications:
    - Word processing, spreadsheet, email, web, etc.

- Customer has some control over the production application:
  - But no control (or worries) about hardware, OS, etc.
  - No expense for maintaining a data center

Infrastructure as a Service (IaaS)

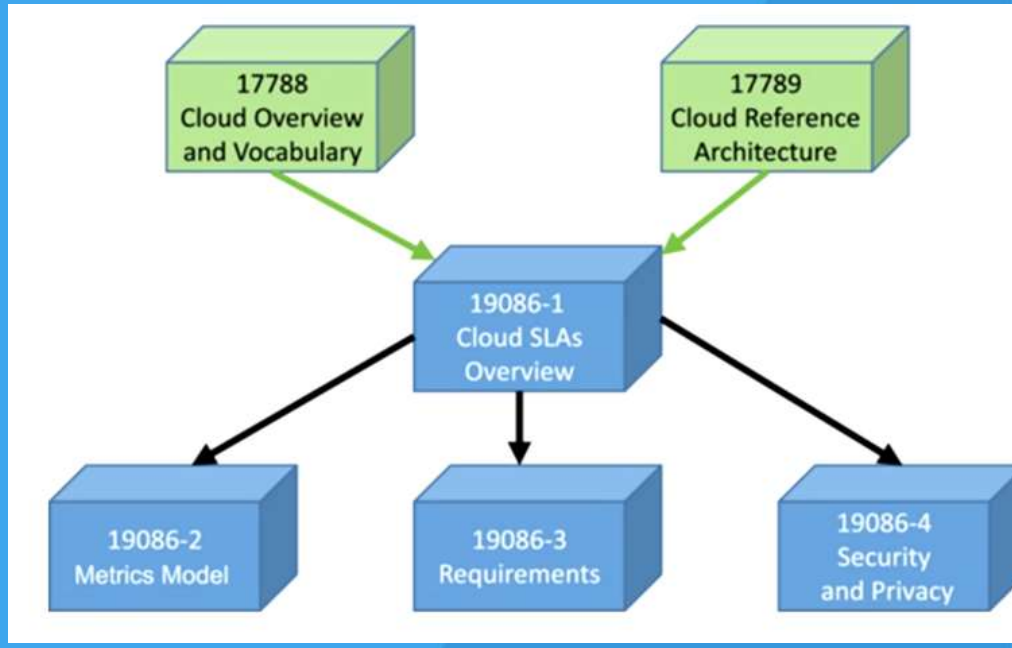
- Cloud provider supplies and manages:
  - Hardware and maybe the core OS
  - Provides data storage capability
- Customer manages the system as though it were in their own data center:
  - Replicates how Admins administer systems they own
- Customer has a fairly high degree of control:
  - And greater responsibility in managing the system
  - Responsibility for maintenance (main difference between PaaS and IaaS) and keeping things up-to-date and running properly
  - It is still much cheaper than maintaining an entire data center

Cloud Security

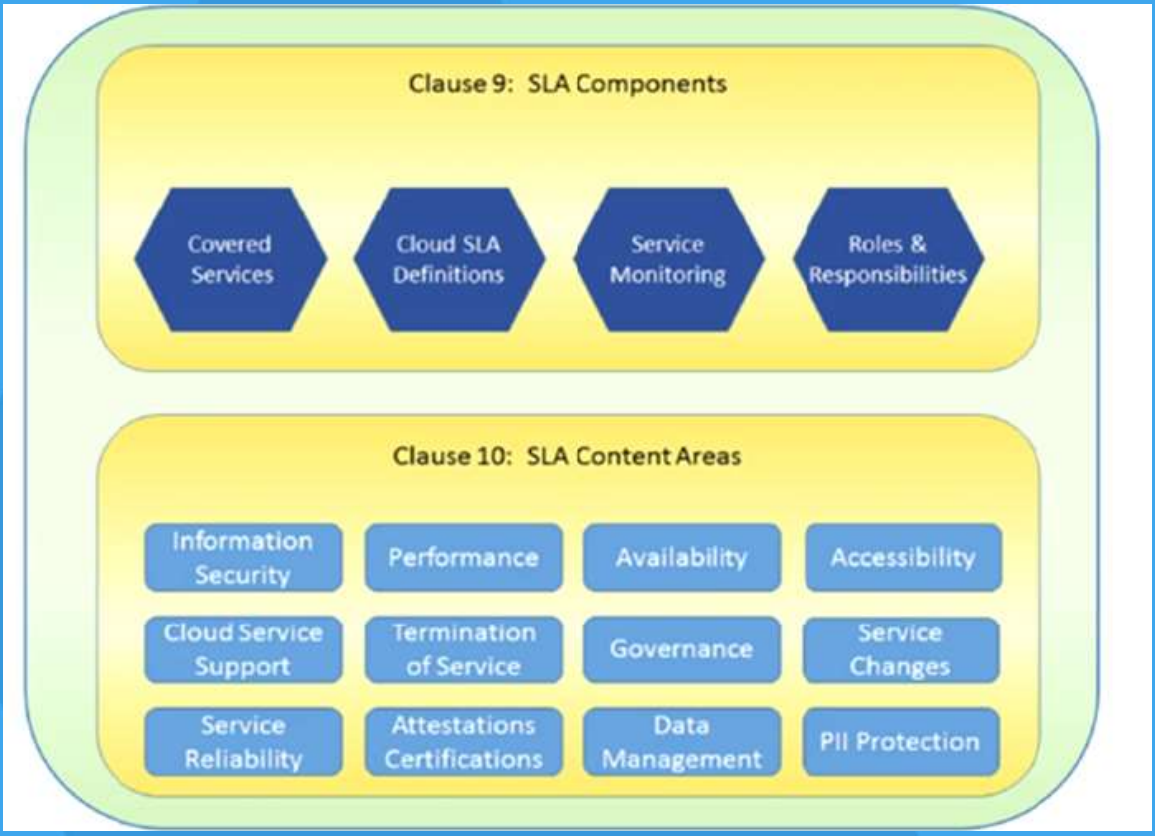
- The problem can be summed up simply
- Your sensitive data is in the control of a third party:
  - You don't know if they are performing good security on that data
- You should choose carefully what data you store/process in the cloud:
  - Proprietary/highly sensitive data should not be stored there
  - UNLESS encrypted prior to storage (zero-knowledge)

Cloud Security: ISO Standards

- ISO 17788: Cloud Overview and Vocabulary (2009)
- ISO 17789: Cloud Reference and Architecture (2009)
- ISO 19086-1: Service Level Agreement Framework (2016)
  - ISO 19086-2b Metric Model, 3 Requirements, and 4 Security and Privacy which are still in draft



ISO 19086-2: SLA Concerns



ISO 19086-2 gives very thorough guidance on questions to ask and answers to obtain before putting your data in the cloud.

Or, if your data is already there, you should still ask these questions now!

Backup Criteria

- Copy on separate media
- If the copy is on the same media as the original, it is a copy (but not a backup)
- Needed when (not if) the original is lost
- To restore the information
- Must be easy to use:
  - Including automatic verification of data integrity
- Should have periodic test recovery

A *backup* is a copy of information that is stored on media separate from the original.

Generally: Greater physical separation = greater security.

Types of Backups: full, incremental and differential

1. Full:
   - Complete dump of data
   - Restore full set from date of creation
   - File system backup versus disk image backup:
     - **File system backup**: the backup software traverses all the directories and files in the file system and systematically copies them to the backup location
     - **Disk image backup**: examines each sector of the physical disk and copies them intact to the backup media, including unused sectors and slack space

Types of Backups: full, incremental and differential

1. Full:
   - Restoring **file system backup** versus Restoring **disk image backup**
   - Type of backup you used can affect what you have at the end of the restore
     - **Restore a file system backup**: Any files on the target device with the same name and location as on the backup will get overwritten
       - Newly created files on the target device will continue to exist
     - **Restore disk image backup**: each sector on the target is overwritten with the data from the backup.
       - Newly created files on the target device will be gone after the restoration completes
   - Disadvantage: huge amounts of backup media (depending of the size of the system being backed up).

Types of Backups

2. Incremental:
   - Dump of data since last backup
   - Restore last full backup and then successive incremental backups

Backup: less space
Restore: low speed

3. Differential:
   - Dump of data since last full backup
   - Restore last full backup and then most recent differential backup

Backup: more space
Restore: high speed

➢ What's more important: Cost, speed, or convenience? (trade-offs)

Backing Up Systems, Applications and Data

- Full system dump:
  - Quick and easy
  - Restores operating system, applications, settings, data ...
    - Returns the system to a prior state
  - Difficult to restore just a portion but that is not usually what you want anyway

For example, Mac "Time Machine"

- Hourly backup for 24 hours
- Daily backup for the last month
- Weekly backup for prior months as long as space allows
- Provides restore back to bootup with configuration and data as of the last backup

- Windows 10 Backup and Restore with File History has a similar capability

Backups Location

- On-site:
  - Fast retrieval
  - Space requirements may outgrow availability
  - Disaster can wipe out backups
- Off-site (yours or someone else's):
  - Data is safe from disaster (at your site!)
  - Slower retrieval
  - Cost and location considerations
- Hybrid:
  - Backups are stored at different locations depending on their age
  - Recent backups on-site (tapes from the past two weeks or month)
  - Long-term storage off-site (because the company is less likely to need that on a regular basis)

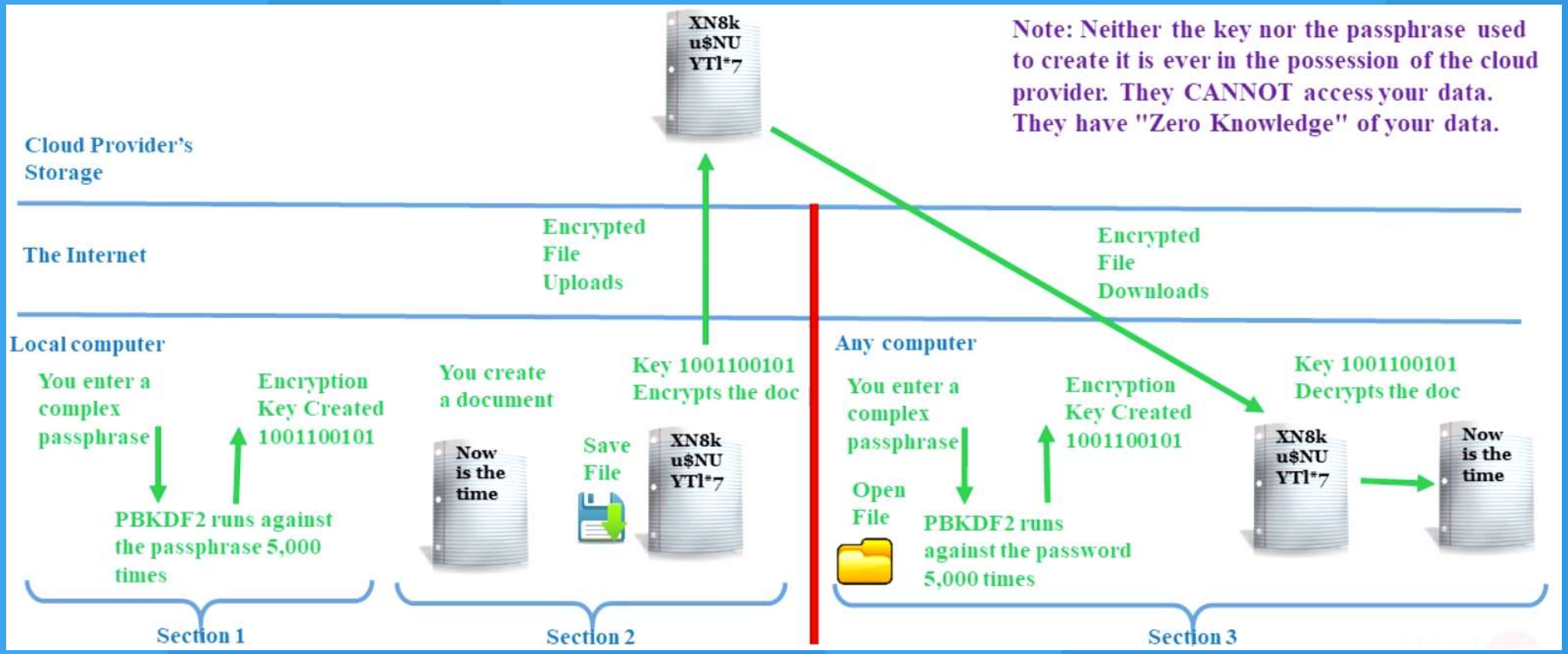
Cloud Based Backup

- You own the information, but not the app:
  - You are reliant on the provider's security measures
  - Can you obtain your data before changing providers?
- Internet is required to access your data:
  - Potential problem in disaster scenarios
- All your data is now on someone else's systems:
  - You MUST use ***zero-knowledge*** if the data is sensitive

Zero-Knowledge:The data encrypts on the local system and only the data copies into the cloud. The cloud provider never has access to the encryption key.

To guard against ransomware, ensure the cloud-based backup supports "versioning"!

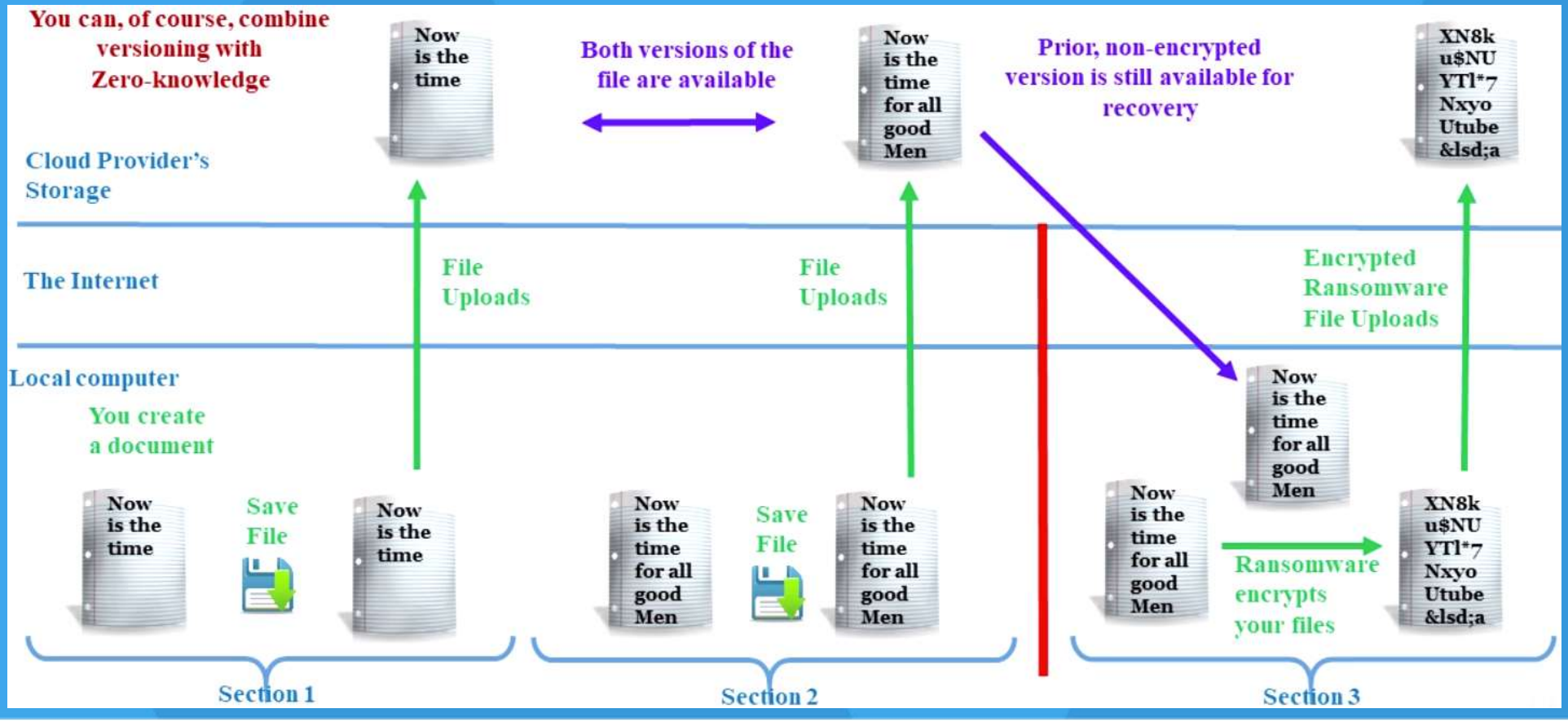
Zero-Knowledge Cloud Storage



Password-Based Key Derivation Function 2 (PBKDF2)

Zero-knowledge application installed

Versioning Backups and Cloud Backup




Questions
& Answers

References

www.sans.org