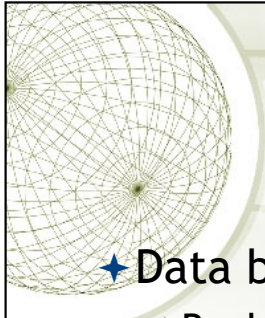




Fundamental Concepts of Data Security

Security Systems 3

Note: This is expected to be delivered over three lectures/workshops



Securing Data

- ★ Data backup
 - ★ Backup technologies
 - ★ Frequency of backup
- ★ Data masking
 - ★ Masking techniques
 - ★ Static vs dynamic
- ★ Secure data erasure

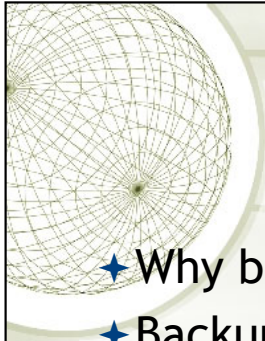
2

Several topics of importance in today's data security:

Data backup

Data masking

Data erasure



Data Backup

- ★ Why backup?
- ★ Backup vs archive
- ★ Backup technologies
 - ✦ Local backup
 - ✦ Server backup
 - ✦ Enterprise backup
 - ✦ Serverless backup (storage area network - SAN)

3

From <https://en.wikipedia.org/wiki/Backup>


*In information technology, a backup, or data backup is a copy of computer data taken and stored elsewhere so that it may be used to **restore the original after a data loss event**. The verb form, referring to the process of doing so, is "back up", whereas the noun and adjective form is "backup". Backups can be used to recover data after its loss from data deletion or corruption, or to recover data from an earlier time. Backups provide a simple form of disaster recovery; however not all backup systems are able to reconstitute a computer system or other complex configuration such as a computer cluster, active directory server, or database server.*

Note the difference between backup and archiving: backup operations protect active data that's changing on a frequent basis whilst archiving operations produces a collection of historical records that are kept for long-term retention and used for future reference.

Data have become one of the most critical assets to nearly all organizations. These data may include financial spreadsheets,

blueprints on new products, customer information, product inventory, trade secrets, and more.

Data usually changes more often than hardware and software, so these backup or archival procedures must happen on a continual basis. The data backup process must make sense and be reasonable and effective. If data in the files changes several times a day, backup procedures should happen a few times a day or nightly to ensure all the changes are captured and kept. If data is changed once a month, backing up data every night is a waste of time and resources. Backing up a file and its corresponding changes is usually more desirable than having multiple copies of that one file. Online backup technologies usually have the changes to a file made to a transaction log, which is separate from the original file.



Local Backup

- ✦ Takes more media
- ✦ Users may have to be relied to do their own backups
- ✦ Less bandwidth taken
- ✦ HDD, Tape, CD, DVD etc.



Server Backup

- ★ Back up data on a local or centralized server
- ★ The local file server stores most or all of the data of the enterprise
- ★ Data made available to clients via the LAN, using common IP network protocols (e.g. NFS, FTP, or CIFS)
- ★ Backup applications protect data on the local server by making copies of the data directly to the local backup system.
- ★ Cons
 - Takes more bandwidth
 - Users must copy data to server
 - Limited data growth



Enterprise Backup

- ★ Enterprise-wide network clients automatically move backup data, via a network, to a backup drive connected to a backup server.
- ★ Automated libraries with multiple backup drives allow multiple backup streams to be received from multiple clients in parallel.
- ★ Backup clients are deployed on every system or workstation and send data on a schedule
- ★ Cons
 - ◆ More bandwidth
 - ◆ More expensive
 - ◆ Still limited with data growth



Server-less Backup

- ✦ Data is moved via a separate backup network or fibre channel SAN directly from disk to tape
- ✦ Only the main servers are connected to these fast and expensive networks
- ✦ Workstations are connected via the TCP/IP network and data is written from the client directly to a tape drive via the relatively slow, but much cheaper, LAN.
- ✦ A server must be involved in initiating and controlling the data moving over the SAN
- ✦ Cons
 - Very expensive

7

See for example https://en.wikipedia.org/wiki/Storage_area_network for further information

A storage area network (SAN) or storage network is a computer network which provides access to consolidated, block-level data storage. SANs are primarily used to enhance accessibility of storage devices, such as disk arrays and tape libraries, to servers so that the devices appear to the operating system as locally-attached devices. A SAN typically is a dedicated network of storage devices not accessible through the local area network (LAN) by other devices, thereby preventing interference of LAN traffic in data transfer.

A SAN does not provide file abstraction, only block-level operations. However, file systems built on top of SANs do provide file-level access, and are known as shared-disk file systems.



Backup Types

★ Full backup

- ★ Everything except swap files
- ★ Not very efficient with media or time
- ★ Usually performed weekly

★ Differential backup

- ★ Only files modified since last full backup
- ★ Archive bits must exist for each file and directory

★ Incremental backup

- ★ All the files that have changed since the last full or incremental backup and sets the archive bit to 0
- ★ Usually performed daily
- ★ More efficient on network traffic, time and media

8

The first step is to do a **full backup**, which is just what it sounds like—all data are backed up and saved to some type of storage media. During a full backup, the archive bit is cleared, which means that it is set to 0. A company can choose to do full backups only, in which case the restoration process is just one step, but the backup and restore processes could take a long time. Most companies choose to combine a full backup with a differential or incremental backup.

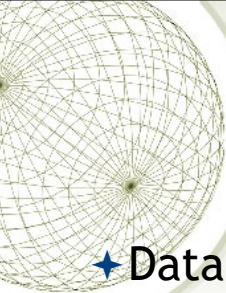
A **differential process** backs up the files that have been modified since the **last full backup**. When the data need to be restored, the full backup is laid down first, and then the most recent differential backup is put down on top of it. The differential process does not change the archive bit value.

An **incremental process** backs up all the files that have changed since the **last full or incremental backup** and sets the archive bit to 0. When the data need to be restored, the full backup data are laid down, and then each incremental backup is laid down on top of it in the proper order. If a company experienced a disaster and it used the incremental process, it would first need to restore the full backup on its hard drives

and lay down every incremental backup that was carried out before the disaster took place (and after the last full backup). So, if the full backup was done six months ago and the operations department carried out an incremental backup each month, the restoration team would restore the full backup and start with the older incremental backups taken since the full backup and restore each one of them until they were all restored.

Note (From Wikipedia https://en.wikipedia.org/wiki/Archive_bit)

The archive bit is a file attribute used by Microsoft operating systems, OS/2, and AmigaOS. It is used to indicate whether or not the file has been backed up (archived). In Windows and OS/2, when a file is created or modified, the archive bit is set (i.e. turned on), and when the file has been backed up, the archive bit is cleared (i.e. turned off). Thus, the meaning of the archive bit is "this file has not been archived". An incremental backup task may use the archive bit to distinguish which files have already been backed up, and select only the new or modified files for backup.



What to back up?

- ★ Data files
- ★ Domain or tree databases
- ★ Domain controller registries
- ★ Don't bother with
 - ★ program files?
 - ★ temp files
 - ★ non critical files
 - ★ seldom changed files



Rotation

- ★ Retention period

- ★ how far back do you want to keep

- ★ Minimum rotation

- ★ two media sets, rotate on each backup

- ★ Light Security rotation

- ★ four media sets, labeled "Mon", "Wed", "Fri 1" and "Fri 2". Starting on the first Friday, a full backup is done to "Fri 1", and then it is stored off-site

- ★ Medium Security rotation

- ★ daily backups with rotating sets
- ★ weekly backups with rotating set



Offsite Storage and Vaulting

- Electronic vaulting: backup via third party
- It is regular and automatic
- Specialised centers against computing and physical disaster
- 24x7 monitoring and user support
- Issues:
 - Who has access
 - Speed
 - Natural disaster protection
 - Intrusion detection/security
 - Encryption/transfer
 - Guarantees

11

Electronic vaulting and remote journaling are other solutions that companies should be aware of. **Electronic vaulting** makes copies of files as they are modified and periodically transmits them to an offsite backup site. The transmission does not happen in real time, but is carried out in batches. So, a company can choose to have all files that have been changed sent to the backup facility every hour, day, week, or month. The information can be stored in an offsite facility and retrieved from that facility in a short time. This form of backup takes place in many financial institutions, so when a bank teller accepts a deposit or withdrawal, the change to the customer's account is made locally to that branch's database and to the remote site that maintains the backup copies of all customer records.

Electronic vaulting is a method of transferring bulk information to offsite facilities for backup purposes. **Remote journaling** is another method of transmitting data offsite, but this usually only includes moving the journal or transaction logs to the offsite facility, not the actual files. These logs contain the deltas (changes) that have taken place to the individual files. If and when data are corrupted and need to be restored, the bank can retrieve these logs, which are used to rebuild the lost data. Journaling is efficient for database recovery, where only the

reapplication of a series of changes to individual records is required to resynchronize the database.



Backup Issues

- Size needed
- Speed needed
- Cost - (often cost per terabyte)
- Automation
- Software conflicts
- Backup software compatibility with OS
- Locked or open files
- Tape life
- Topology
- Always perform data verification



Secure Data Erasure

★ Why

- ★ Confidentiality issue
- ★ Media flow in/out of organisation

★ Key

- ★ Information classification
- ★ Media types
- ★ Software based
- ★ Hardware based
- ★ Verifiable

13

FROM NIST SP800-80

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-88.pdf>

Media sanitization is one key element in assuring **confidentiality**. In order for organizations to have appropriate controls on the information they are responsible for safeguarding, they must properly safeguard used media. An often rich source of illicit information collection is either through dumpster diving for improperly disposed hard copy media, acquisition of improperly sanitized electronic media, or through keyboard and laboratory reconstruction of media sanitized in a manner not commensurate with the confidentiality of its information. Media flows in and out of organizational control through recycle bins in paper form, out to vendors for equipment repairs, and hot swapped into other systems in response to emergencies. This potential vulnerability can be mitigated through proper understanding of where information is location, what that information is and how to protect it.

The key in deciding how to manage media in an organization is to first consider the information, then the media type. In organizations,

information exists that is not associated with any categorized system. This information is often hard copy internal communications such as memoranda, white papers, and presentations. Sometimes this information may be considered sensitive. Examples may include internal disciplinary letters, financial or salary negotiations, or strategy meeting minutes. Organizations should label these media with their internal operating classifications and associate a type of sanitization described in this publication.



Secure Data Erasure

❖ Categories

- ❖ Disposal: no consideration
- ❖ Clearing: against keyboard attack
- ❖ Purging: against laboratory attack
- ❖ Destroying: media cannot be reused

14

FROM NIST SP800-80


<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-88.pdf>

There are different types of sanitization for each type of media. We have divided media sanitization into four categories:

- Disposal: discarding media with no other sanitization considerations
- Clearing: a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack, e.g. overwriting
- Purging: a media sanitization process that protects the confidentiality of information against a laboratory attack, e.g. executing firmware secure erase command, degaussing hard drives
- Destroying: destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting.

Organizations should consider the following environmental factors. Note that the list is not all-inclusive:

- What types (e.g., optical non-rewritable, magnetic) and size (e.g., megabyte, gigabyte, and terabyte) of media storage does the organization require to be sanitized?
- What is the confidentiality of the data stored on the media?
- Will the media be processed in a controlled area?
- Should the sanitization process be conducted within the organization or outsourced?
- What is the anticipated volume of media to be sanitized by type of media? 1
- What is the availability of sanitization equipment and tools?
- What is the level of training of personnel with sanitization equipment/tools?
- How long will sanitization take?
- What type of sanitization will cost more considering tools, training, validation, and re-entering media into the supply stream?



Data Masking

- ★ What
 - ★ Process of hiding original classified data
 - ★ Same format, different values
- ★ Where
 - ★ Testing applications/systems
 - ★ Training
 - ★ Third-party analytics
 - ★ Security requirements (invisible to operators)

15

Process of hiding original data with random characters or data.

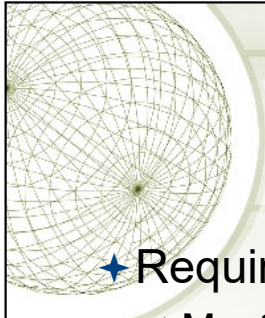
The main reason for applying masking to a data field is to protect data that is classified as personal identifiable data, personal sensitive data or commercially sensitive data, however the data must remain usable for the purposes of undertaking valid test cycles. It must also look real and appear consistent. It is more common to have masking applied to data that is represented outside of a corporate production system. In other words, where data is needed for the purpose of application development, building program extensions and conducting various test cycles. It is common practice in enterprise computing to take data from the production systems to fill the data component, required for these non-production environments. However the practice is not always restricted to non-production environments. In some organizations, data that appears on terminal screens to call centre operators may have masking dynamically applied based on user security permissions. (e.g.: Preventing call centre operators from viewing Credit Card Numbers in billing systems)

The primary concern from a corporate governance perspective is that

personnel conducting work in these non-production environments are not always security cleared to operate with the information contained in the production data. This practice represents a security hole where data can be copied by unauthorised personnel and security measures associated with standard production level controls can be easily bypassed. This represents an access point for a data security breach.

The overall practice of Data Masking at an organisational level should be tightly coupled with the Test Management Practice and underlying Methodology and should incorporate processes for the distribution of masked test data subsets.

https://en.wikipedia.org/wiki/Data_masking



Data Masking

- ★ Requirements
 - ★ Must remain usable for testing purposes.
 - ★ Must look real and appear consistent.
 - ★ Not able to be reverse engineered.
 - ★ Must remain meaningful, e.g. credit card validation
 - ★ Must have sufficient changes to the original data

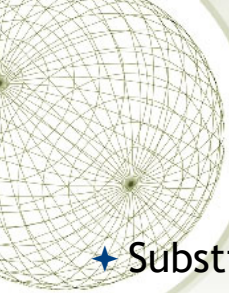
16

Data involved in any data-masking or obfuscation must remain meaningful at several levels:

The data must remain meaningful for the application logic. For example, if elements of addresses are to be obfuscated and city and suburbs are replaced with substitute cities or suburbs, then, if within the application there is a feature that validates postcode or post code lookup, that function must still be allowed to operate without error and operate as expected. The same is also true for credit-card algorithm validation checks and Social Security Number validations.

The data must undergo enough changes so that it is not obvious that the masked data is from a source of production data. For example, it may be common knowledge in an organisation that there are 10 senior managers all earning in excess of \$300K. If a test environment of the organisation's HR System also includes 10 identities in the same earning-bracket, then other information could be pieced together to reverse-engineer a real-life identity. Theoretically, if the data is obviously masked or obfuscated, then it would be reasonable for someone intending a data breach to assume that they could reverse engineer

identity-data if they had some degree of knowledge of the identities in the production data-set. Accordingly, data obfuscation or masking of a data-set applies in such a manner as to ensure that identity and sensitive data records are protected - not just the individual data elements in discrete fields and tables.



Data Masking Techniques

- ★ Substitution
 - ★ Different authentic value is substituted for existing value
 - ★ Requires large substitution datasets

17

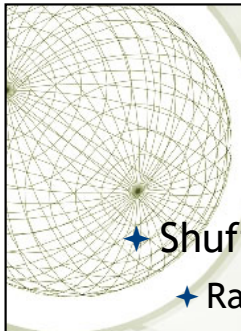
Substitution is one of the most effective methods of applying data masking and being able to preserve the authentic look and feel of the data records. It allows the masking to be performed in such a manner that another authentic looking value can be substituted for the existing value. There are several data field types where this approach provides optimal benefit in disguising the overall data sub set as to whether or not it is a masked data set. For example, if dealing with source data which contains customer records, real life surname or first name can be randomly substituted from a supplied or customised look up file.

If the first pass of the substitution allows for applying a male first name to all first names, then the second pass would need to allow for applying a female first name to all first names where gender equals "F". Using this approach we could easily maintain the gender mix within the data structure, apply anonymity to the data records but also maintain a realistic looking database which could not easily be identified as a database consisting of masked data.

This substitution method needs to be applied for many of the fields that are in DB structures across the world, such as telephone numbers, zip

codes and postcodes, as well as credit card numbers and other card type numbers like Social Security numbers and Medicare numbers where these numbers actually need to conform to a checksum test of the Luhn algorithm.

In most cases the substitution files will need to be fairly extensive so having large substitution datasets as well the ability to apply customised data substitution sets should be a key element of the evaluation criteria for any data masking solution.



Data Masking Techniques

- ★ **Shuffling**
 - ★ Randomly shuffled within the column
 - ★ Should not be used in isolation
- ★ **Number and date variance**
 - ★ +/- 10% can still be meaningful
 - ★ Date shifting
- ★ **Masking out**
 - ★ Similar to nulling out except keeping some of the data intact, e.g. XXXX XXXX XXXX 2345
 - ★ not effective for testing

18

Shuffling

The shuffling method is a very common form of data obfuscation. It is similar to the substitution method but it derives the substitution set from the same column of data that is being masked. In very simple terms, the data is randomly shuffled within the column. However, if used in isolation, anyone with any knowledge of the original data can then apply a "What If" scenario to the data set and then piece back together a real identity. The shuffling method is also open to being reversed if the shuffling algorithm can be deciphered.

Shuffling however has some real strengths in certain areas. If for instance, the end of year figures for financial information in a test data base, one can mask the names of the suppliers and then shuffle the value of the accounts throughout the masked database. It is highly unlikely that anyone, even someone with intimate knowledge of the original data could derive a true data record back to its original values

Number and date variance

The numeric variance method is very useful for applying to financial and date driven information fields. Effectively, a method utilising this manner of masking can still leave a meaningful range in a financial data set such as payroll. If the variance applied is around +/- 10% then it is still a very meaningful data set in terms of the ranges of salaries that are paid to the recipients.

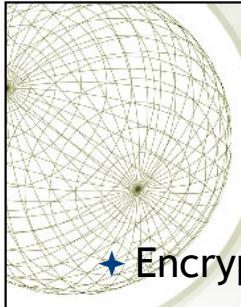
The same also applies to the date information. If the overall data set needs to retain demographic and actuarial data integrity then applying a random numeric variance of +/- 120 days to date fields would preserve the date distribution but still prevent traceability back to a known entity based on their known actual date or birth or a known date value of whatever record is being masked

Masking out

Character scrambling or masking out of certain fields is also another simplistic yet very effective method of preventing sensitive information to be viewed. It is really an extension of the previous method of nulling out but there is greater emphasis on keeping the data real and not fully masked all together.

This is commonly applied to credit card data in production systems. For instance, you may have spoken with an operator in a Call Centre and they have suggested they could bill an item to your credit card. They then quote you a billing reference to your card with the last 4 digits of XXXX XXXX xxxx 6789. As an operator they can only see the last 4 digits of your card number but once the billing system passes your details for charging the full number is revealed to the payment gateway systems.

This system is not very effective for test systems but is very useful for the billing scenario detailed above. It is also commonly known as a dynamic data masking method.



Data Masking Techniques

- ★ Encryption
 - ★ Most complex
 - ★ Requires key base on user rights
 - ★ Not effective
- ★ Nulling out / deletion
 - ★ Simplistic
 - ★ Cannot be used where software requires validation

19

Encryption

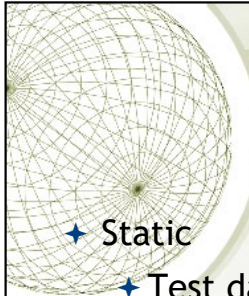
Encryption is often the most complex approach to solving the data masking problem. The encryption algorithm often requires that a "key" be applied to view the data based on user rights. This often sounds like the best solution but in practice the key may then be given out to personnel without the proper rights to view the data and this then defeats the purpose of the masking exercise. Old databases may then be copied with the original credentials of the supplied key and the same uncontrolled problem lives on.

Recently, the problem of encrypting data while preserving the properties of the entities got a recognition and newly acquired interest among the vendors and academia. New challenge gave birth to algorithms called FPE (format preserving encryption). They are based on the accepted AES algorithmic mode that makes them being recognized by NIST

Nulling out or deletion

Sometimes a very simplistic approach to masking is adopted through applying a null value to a particular field. The null value approach is really only useful to prevent visibility of the data element.

In almost all cases it lessens the degree of data integrity that is maintained in the masked data set. It is not a realistic value and will then fail any application logic validation that may have been applied in the front end software that is in the system under test. It also highlights to anyone that wishes to reverse engineer any of the identity data that data masking has been applied to some degree on the data set.



Types of Data Masking

- ★ Static
 - ★ Test data generated from backup of original data
- ★ Dynamic
 - ★ Masking happens at runtime, dynamically and on demand
 - ★ Avoid the need for a second data source to store masked data
- ★ On-The-Fly
 - ★ Copy from original to test environment
 - ★ Good for sharing data
 - ★ One record at a time

20

Static Data Masking is done on the golden copy of the database. Production DBAs load the backup in a separate environment, reduce the data set to a subset that holds the data necessary for a particular round of testing (a technique called "subsetting"), apply data masking rules while data is in stasis, apply necessary code changes from source control and push data to desired environment.

On-the-Fly Data Masking happens in the process of transferring data from environment to environment without data touching the disk on its way. The same technique is applied to "Dynamic Data Masking" but one record at a time. This type of data masking is most useful for environments that do continuous deployments as well as for heavily integrated applications. Organizations that employ continuous deployment or continuous delivery practices do not have the time necessary to create a backup and load it to the golden copy of the database. Thus, continuously sending smaller subsets (deltas) of masked testing data from production is important. In heavily integrated applications, developers get feeds from other production systems at the very onset of development and masking of these feeds is either overlooked and not budgeted until later, making organizations non-compliant. Having on-the-fly data masking in place becomes essential.

Dynamic Data Masking is similar to On-the-Fly Data Masking but it differs in the sense that On-the-Fly Data Masking is about copying data from one source to another source so that the latter can be shared. Dynamic data masking happens at runtime, dynamically, and on-demand so that there need not be a second data source where to store the masked data dynamically.

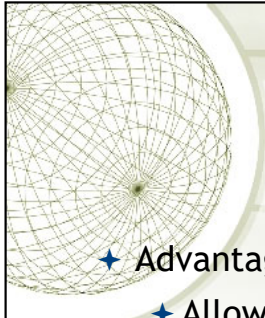
Dynamic data masking enables several scenarios, many of which revolve around strict privacy regulations e.g. the Singapore Monetary Authority or the Privacy regulations in Europe.

Dynamic data masking is attribute-based and policy-driven. Policies include:

- Doctors can view the medical records of patients they are assigned to (data filtering)

- Doctors cannot view the SSN field inside a medical record (data masking).

Dynamic data masking can also be used to encrypt or decrypt values on the fly especially when using format-preserving encryption.



Static vs Dynamic

- ★ Advantages of static data masking
 - ★ Allows the development and testing without influencing live systems
 - ★ Best practice for working with contractors and outsourced developers, DBAs, and testing teams
 - ★ Provides a more in-depth policy of masking capabilities
 - ★ Allows organizations to share the database with external companies

21

A very good article on the Internet to help understand more about the difference between static and dynamic masking

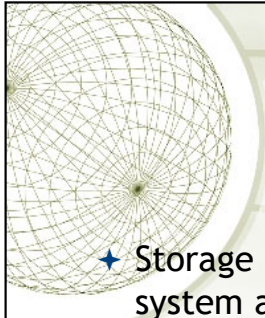
<https://www.imperva.com/blog/static-versus-dynamic-data-masking/>



Static vs Dynamic

- ★ Advantages of dynamic data masking
 - ★ The sensitive information never leaves the database!
 - ★ No changes are required at the application or the database layer
 - ★ Customized access per IP address, per user, or per application
 - ★ No duplicate or off-line database required
 - ★ Activities are performed on real data, saving time and providing real feedback to developers and quality assurance

22



Storage Devices

- ★ Storage devices are a fundamental component of a system and there many types devices available ranging from high capacity hard drives to small capacity USB drives or memory cards.
- ★ Storage devices are critical components from the point of view cyber security. Why?
- ★ Systems can booted from storage devices which can override local settings.

23

Additional Storage Devices

Besides the memory environment discussed previously, many types of physical storage devices should be covered, along with the ramifications of security compromises that could affect them. Many, if not all, of the various storage devices used today enable the theft or compromise of data in an organization. As their sizes have shrunk, their capacities have grown. Floppy disks, while small in relative storage capacity (about 1.44MB of data), have long been known to be a source of viruses and data theft. A thief who has physical access to a computer with an insecure operating system can use a basic floppy disk to boot the system.

Many PCs and Unix workstations have a BIOS that allows the machine to be booted from devices other than the floppy disk, such as a CD-ROM or even a USB thumb drive. Possible ways to harden the environment include password-protecting the BIOS so that a nonapproved medium cannot take over the machine, and controlling access to the physical environment of the computer equipment.

In many instances, removable storage units have unfortunately come up missing. Two noteworthy incidents occurred in July 2004, at which

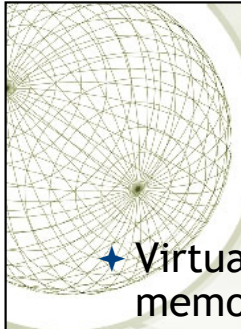
time both Los Alamos National Laboratory and Sandia National Laboratories reported lost storage media containing classified information. This raised enough of a concern at Los Alamos that the military research facility was totally shut down, with no employees allowed to enter, while a thorough search and investigation was performed. Sandia National Laboratories reported it was missing a computer floppy disk marked classified, which it later located.

Rewritable CD/DVDs, mini-disks, optical disks—virtually any portable storage medium—can be used to compromise security. Current technology headaches for the security professional include USB thumb drives and USB-attachable MP3 players capable of storing multiple gigabytes of data. The first step in prevention is to update existing security policies (or implement new ones) to include the new technologies. Even cellular phones can be connected to computer ports for data, sound, image, and video transmission that could be out of bounds of an outdated security policy. Technologies such as Bluetooth, FireWire, and Blackberry all have to be taken into account when addressing security concerns and vulnerabilities.



Storage Devices

- ★ Confidential information can be retrieved by gaining access to the storage devices (which are either discarded without being properly "wiped" or removed from the systems).
- ★ Confidential information can illegally copied via removable media.



Storage Devices

- ★ Virtual memory - used to extend the system memory.
- ★ The access to the virtual memory is slower because of the nature of the storage.
- ★ Problems with virtual memory:
 - a) access to encrypted data
 - b) access to memory contents after the power has been turned off.

25

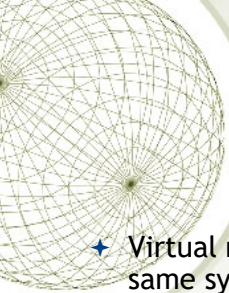
Virtual Memory

Secondary storage is considered nonvolatile storage media and includes such things as the computer's hard drive, floppy disks, and CD-ROMs. When RAM and secondary storage are combined, the result is virtual memory. The system uses hard drive space to extend its RAM memory space. Swap space is the reserved hard drive space used to extend RAM capabilities. Windows systems use the pagefile.sys file to reserve this space. When a system fills up its volatile memory space, it writes data from memory onto the hard drive. When a program requests access to this data, it is brought from the hard drive back into memory in specific units, called pages. This process is called virtual memory paging. Accessing data kept in pages on the hard drive takes more time than accessing data kept in memory because physical disk read/write access must take place. Internal control blocks, maintained by the operating system, keep track of what page frames are residing in RAM and what is available "offline," ready to be called into RAM for execution or processing, if needed. The payoff is that it seems as though the system can hold an incredible amount of information and program instructions in memory.

Paging, pageframes, etc

A security issue with using virtual swap space is that when the system is shut down, or processes that were using the swap space are terminated, the pointers to the pages are reset to “available” even though the actual data written to disk is still physically there. These data could conceivably be compromised and captured. On a very secure operating system, there are routines to wipe the swap spaces after a process is done with it, before it is used again. The routines should also erase this data before a system shut-down, at which time the operating system would no longer be able to maintain any control over what happens on the hard drive surface.

NOTE - If a program, file, or data are encrypted and saved on the hard drive, they will be decrypted when used by the controlling program. While these unencrypted data are sitting in RAM, the system could write out the data to the swap space on the hard drive, in their unencrypted state. Attackers have figured out how to gain access to this space in unauthorized manners.



Virtual Machines

- ★ Virtual machines - enables the running of multiple OSes on the same system.
- ★ Current virtualization software is advanced:
 - a) it allows very effective simulations of OSes - depending on the level of access and hardware support, the virtual machine can be indistinguishable from the actual machine,
 - b) it can be used to simulate large scale systems rather than individual machines - e.g. VMWare allows the user to tailor specific networks of virtual servers and user machines.
- ★ Virtualization is key aspect of cloud computing and poses major challenges in terms of cyber security.

26

Virtual Machines

If you have been into computers for a while, you might remember computer games that did not have the complex, life-like graphics of today's games. Pong and Asteroids were what we had to play with when we were younger. In those simpler times, the games were 16-bit and were written to work in a 16-bit MS-DOS environment. When our Windows operating systems moved from 16-bit to 32-bit, the 32-bit operating systems were written to be backward compatible, so someone could still load and play a 16-bit game in an environment that the game did not understand. The continuation of this little life pleasure was available to users because the operating systems created virtual machines for the games to run in.

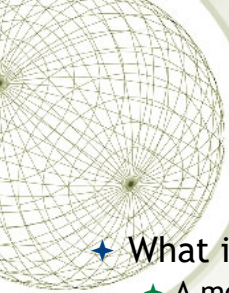
When a 16-bit application needs to interact with the operating system, it has been developed to make system calls and interact with the computer's memory in a way that would only work within a 16-bit operating system—not a 32-bit system. So, the virtual machine simulates a 16-bit operating system, and when the application makes a request, the operating system converts the 16-bit request into a 32-bit request (this is called thunking) and reacts to the request appropriately. When the system sends a reply to this request, it changes the 32-bit

reply into a 16-bit reply so the application understands it.

Today, virtual machines are much more advanced. Basic virtualization enables single hardware equipment to run multiple operating system environments synchronously, greatly enhancing processing power utilization, among other benefits. Creating virtual instances of operating systems, applications, and storage devices is known as virtualization.

In today's jargon, a virtual instance of an operating system is known as a virtual machine. A virtual machine is commonly referred to as a guest that is executed in the host environment. Virtualization allows a single host environment to execute multiple guests at once, with multiple virtual machines dynamically pooling resources from a common physical system. Computer resources such as RAM, processors, and storage are emulated through the host environment. The virtual machines do not directly access these resources; instead, they communicate with the host environment responsible for managing system resources.

What this means is that you can have one computer running several different operating systems at one time. For example, you can run a system with Windows 2000, Linux, Unix, and Windows 2008 on one computer. Think of a house that has different rooms. Each operating system gets its own room, but each share the same resources that the house provides—a foundation, electricity, water, roof, and so on. An operating system that is “living” in a specific room does not need to know about or interact with another operating system in another room to take advantage of the resources provided by the house. The same concept happens in a computer: Each operating system shares the resources provided by the physical system (as in memory, processor, buses, and so on). They “live” and work in their own “rooms,” which are the guest virtual machines. The physical computer itself is the host.



Virtualization and Cloud Computing

- ★ What is cloud computing?
 - ★ A model which enables the combination of hardware, software, networking that allows the delivery of on-demand computing resources via the Internet or private network.
- ★ What are the categories of cloud solutions?
 - ★ Public cloud
 - ★ Community cloud
 - ★ Private cloud
 - ★ Hybrid cloud

27

What is cloud computing?

An IT model or computing environment composed of IT components (hardware, software, networking, and services) as well as the processes around the deployment of these elements that together enable us to develop and deliver cloud services via the Internet or a private network.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. In its simplest definition, a public cloud exists externally to its end user and is generally available with little restriction as to who may pay to use it. As a result, the most common forms of public clouds are ones that are accessed via the Internet. There has been tremendous development in the public cloud space, resulting in very sophisticated Infrastructure-as-a-Service offerings from companies like Amazon, with their Elastic Compute Cloud (EC2), Rackspace's Cloud Offerings, and IBM's BlueCloud. Other forms of public cloud offerings can take the form at more of the application layer, or Platform-as-a-Service, like Google's AppEngine and Windows' Azure Services

platform, as well as Amazon's service-specific cloud hosting SimpleDB, Cloud Front, and S3 Simple Storage.

At a basic level, public clouds have unique security components and evaluation criteria when compared with private clouds. Public clouds can be formed by service providers wishing to build out a high-capacity infrastructure and lease pieces of it to a variety of clients. As a result, data might become comingled on common storage devices, making identity, access control, and encryption very important. There is a certain amount of inherent trust (albeit it should be a measured, tested, and verified) by subscribers with their public cloud providers.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise. The promise of community clouds is that they allow multiple independent entities to gain the cost benefits of a shared nonpublic cloud while avoiding security and regulatory concerns that might be associated with using a generic public cloud that did not address such concerns in its SLA. This model has tremendous potential for entities or companies that are subject to identical regulatory, compliance, or legal restrictions. Different kinds of community clouds are being considered in the United States and the European Union by governments at the national and local levels. This makes great sense since there are multiple benefits to both the individual entities as well as collectively. For instance, when multiple government agencies that transact business with each other have their processing colocated in a single facility, they can achieve both savings and increased security in terms of reducing the amount of traffic that would otherwise need to traverse the Internet. Continuity of operations can also be enhanced at a lower overall cost to all parties when multiple data centers are used to implement such a community cloud.

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. In contrast to a public cloud, a private cloud is internally hosted. The hallmark of a private cloud is that it is usually dedicated to an organization. Although there is no comingling of data or sharing of resources with external entities, different departments within the organization may have strong requirements to maintain data isolation within their shared private cloud. Organizations deploying private clouds often do so utilizing

virtualization technology within their own data centers. A word of caution here:

“Describing private cloud as releasing you from the constraints of public cloud only does damage to the cloud model. It’s the discipline in cloud implementations that makes them more interesting (and less costly) than conventional IT. Private clouds could very well be more constrained than their public counterparts and probably will be to meet those needs that public clouds cannot address.”

Since private clouds are, well, private, some of the security concerns of a public cloud may not apply. However, just because they are private does not mean that they are necessarily more secure. In a private cloud, considerations such as securing the virtualization environment itself (that is, hypervisor level security, physical hardware, software, and firmware, and so on) must still be addressed, whereas in a public cloud, you would rely on the provider to do so. As a result, when comparing public to private clouds, it may be difficult to make generalizations as to which is inherently more secure. But as we pointed out earlier in this chapter in the section on Control over Security in the Cloud Model, a private cloud offers the potential to achieve greater security over your cloud-based assets. However, between the potential for better security and the achievement of better security lie many ongoing activities. The true advantage of a private cloud is that “the provider has a vested interest in making the service interface more perfectly matched to the tenant needs.” However, it should also be pointed out that many of the sins of enterprise security have to do with the fact that the enterprise itself implements and manages its own IT security—which would be perfectly fine except security is generally not a core investment nor is it measured as though it were.

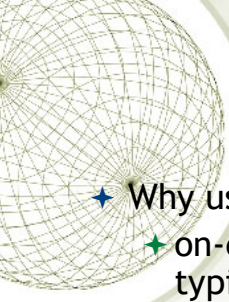
Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). Hybrid clouds are just as the name implies. They are formed when an organization builds out a private cloud and wishes to leverage public or community clouds in conjunction with its private cloud for a particular purpose; the linking of the two clouds is what would be called a hybrid cloud. (Actually, a hybrid cloud could be formed by any combination of the three cloud types: public, private, and community.)

Many organizations deploy an internal private cloud for their critical

infrastructure but find certain needs that just aren't economical to build out internally. A common example would be for testing or quality assurance purposes. For instance, an internal cloud might be used to run the infrastructure of a business, but the business may need to test an upgrade or roll out of a new system. It might be advantageous to pay for capacity of a public cloud for a few months to complete the testing, and when their own private cloud is upgraded, discontinue the public cloud usage.

Another example of a hybrid cloud would be a Web site where its core infrastructure is private to the company, but certain components of the Web site are hosted externally—that is, heavily trafficked media such as streaming video or image caching.

If an organization has already built out an internal cloud, additional advantages of public cloud-based architectures may be too great to ignore. As a result, many organizations may consider the benefits of adopting a public-private hybrid model. However, certain requirements can prevent hybrid clouds from being fully adopted by an organization. For instance, financial services organizations might not be able to meet specific compliance regulations if customer data is externally hosted at a third party, no matter how well it may be secured. Governments might not be able to take the risk of the compromise (political, malicious, or otherwise) if their cloud-based data is attacked. Yet all these organizations might still have specific use cases for public clouds.



Virtualization and Cloud Computing

- ★ Why use the cloud?
 - ★ on-demand storage and processing resources at typically lower cost
 - ★ dedicated security comes as part of the typical cloud solution
- ★ Cloud services
 - ★ Infrastructure-as-a-Service (IaaS): e.g. Amazon AWS, Microsoft Azure
 - ★ Platform-as-a-Service (PaaS): e.g. Google Cloud Platform, Microsoft ML studio
 - ★ Software-as-a-Service (SaaS): e.g. GoogleDoc, Gmail, Office365

28

Cloud Platform-as-a-Service

PaaS providers usually deliver a bundling of software and infrastructure in the form of a programmable container and provide a cloud for an end user to host their own developed applications or services. PaaS is similar to SaaS, but with PaaS, the service is the entire application environment—typically, PaaS includes the computing platform as well as the development and solution stack.

Google's Google App Engine is an excellent example of a PaaS architecture. So is Salesforce.com's Force.com platform. In both cases, the end user receives an environment from the provider (also called a container) that is ready to host a particular application or service that the end user requires. The end user does not need to worry about lower-level services such as the infrastructure; these are provided for them within the service.

Cloud Infrastructure-as-a-Service

In general, IaaS clouds deliver virtualized resources, such as guest virtual machines (ready to load an operating system), storage, or database services. The tenant interacts with IaaS clouds in a similar way as giving a systems architecture to an IT department to provide the

necessary systems (although usually with very formal descriptions). This is the virtual equivalent to physically deploying servers, storage, or database.

Amazon's Web Services or RackSpace's Cloud Services are both prime examples of IaaS providers. In their most common form, end users choose to still have the ability to manage their infrastructure at the operating system level but out-source as-a-service the details of managing and maintaining the servers, switching, routing, firewalling, and connectivity concerns. They basically purchase this bundled from the IaaS provider.

Cloud Software-as-a-Service

In its most common form, a SaaS cloud implementation delivers software or, more generally described, an application to its end user. The end user doesn't usually need to understand or be concerned with the supporting infrastructure and simply utilizes an application. All the back office details of the application are masked and provided as-a-service behind the scenes of that application.

Web sites accessed via the Internet that provide the end user an application or a service can be considered SaaS. For instance, Salesforce.com provides a CRM SaaS, Google's GMAIL or Yahoo Mail provide email services, and even former premise-based software-only solutions like Microsoft Share Point are available as SaaS online, via a Web browser.

There are several important security concerns we need to address in considering the use of virtualization for cloud computing. One potential new risk area has to do with the potential to compromise a virtual machine hypervisor itself. If the hypervisor is vulnerable to being exploited, it will become a primary target. At the scale of a cloud, such a risk would have broad impact if not otherwise mitigated with network isolation and if it is not detected by security monitoring.

What is a hypervisor?

Hypervisors are purpose-built software with a small and specific set of functions. A hypervisor is smaller, more focused than a general purpose operating system, and less exposed, having fewer or no externally accessible network ports. A hypervisor does not undergo frequent change and does not run third-party applications. The guest operating systems, which may be vulnerable, do not have direct access to the hypervisor. In fact, the hypervisor is completely transparent (invisible) to network traffic with the exception of traffic to/from a dedicated hypervisor management interface. Furthermore, at present there are no documented attacks against hypervisors, reducing the

likelihood of attack.

Network Availability The value of cloud computing can only be realized when your network connectivity and bandwidth meet your minimum needs: The cloud must be available whenever you need it. If it is not, then the consequences are no different than a denial-of-service situation.

Cloud Provider Viability Since cloud providers are relatively new to the business, there are questions about provider viability and commitment. This concern deepens when a provider requires tenants to use proprietary interfaces, thus leading to tenant lock-in.

Disaster Recovery and Business Continuity Tenants and users require confidence that their operations and services will continue if the cloud provider's production environment is subject to a disaster.

Security Incidents Tenants and users need to be appropriately informed by the provider when an incident occurs. Tenants or users may require provider support to respond to audit or assessment findings. Also, a provider may not offer sufficient support to tenants or users for resolving investigations.

Transparency When a cloud provider does not expose details of their internal policy or technology implementation, tenants or users must trust the cloud provider's security claims. Even so, tenants and users require some transparency by providers as to provider cloud security, privacy, and how incidents are managed.

Loss of Physical Control Since tenants and users lose physical control over their data and applications, this results in a range of concerns:

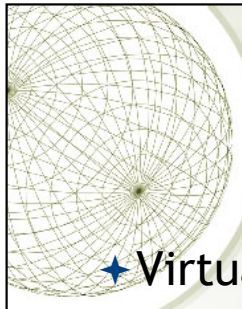
Privacy and Data With public or community clouds, data may not remain in the same system, raising multiple legal concerns.

Control over Data User or organization data may be comingled in various ways with data belonging to others.

A tenant administrator has limited control scope and accountability within a Public infrastructure-as-a-service (IaaS) implementation, and even less with a platform-as-a-service (PaaS) one.

Tenants need confidence that the provider will offer appropriate control, while recognizing that tenants will simply need to adapt their expectations for how much control is reasonable within these models.

New Risks, New Vulnerabilities There is some concern that cloud computing brings new classes of risks and vulnerabilities. Although we can postulate various hypothetical new risks, actual exploits will largely be a function of a provider's implementation. Although all software, hardware, and networking equipment are subject to unearthing of new vulnerabilities, by applying layered security and well-conceived operational processes, a cloud may be protected from common types of attack even if some of its components are inherently vulnerable.



Cloud Computing Issues

- ★ Virtualization issues, e.g. hypervisors
- ★ Network availability
- ★ Cloud provider viability
- ★ Security incidents
- ★ Transparency

29

There are security issues with Cloud Computing, below are some common issues:

Compromised Hypervisors:

There are several important security concerns we need to address in considering the use of virtualization for cloud computing. One potential new risk area has to do with the potential to compromise a virtual machine hypervisor itself. If the hypervisor is vulnerable to being exploited, it will become a primary target. At the scale of a cloud, such a risk would have broad impact if not otherwise mitigated with network isolation and if it is not detected by security monitoring.

What is a hypervisor? hypervisors are purpose-build software with a small and specific set of functions. A hypervisor is smaller, more focused than a general purpose operating system, and less exposed, having fewer or no externally accessible network ports. A hypervisor does not undergo frequent change and does not run third-party applications. The guest operating systems, which may be vulnerable, do not have direct access to the hypervisor. In fact, the hypervisor is completely transparent (invisible) to network traffic with the exception of

traffic to/from a dedicated hypervisor management interface. Furthermore, at present there are no documented attacks against hypervisors, reducing the likelihood of attack.

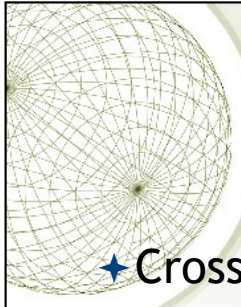
Network Availability The value of cloud computing can only be realized when your network connectivity and bandwidth meet your minimum needs: The cloud must be available whenever you need it. If it is not, then the consequences are no different than a denial-of-service situation.

Cloud Provider Viability Since cloud providers are relatively new to the business, there are questions about provider viability and commitment. This concern deepens when a provider requires tenants to use proprietary interfaces, thus leading to tenant lock-in.

Disaster Recovery and Business Continuity Tenants and users require confidence that their operations and services will continue if the cloud provider's production environment is subject to a disaster.

Security Incidents Tenants and users need to be appropriately informed by the provider when an incident occurs. Tenants or users may require provider support to respond to audit or assessment findings. Also, a provider may not offer sufficient support to tenants or users for resolving investigations.

Transparency When a cloud provider does not expose details of their internal policy or technology implementation, tenants or users must trust the cloud provider's security claims. Even so, tenants and users require some transparency by providers as to provider cloud security, privacy, and how incidents are managed.



Cloud Computing Issues

- ★ Cross VM traffic
- ★ Cloud data storage
- ★ Loss of physical control
- ★ New risks new vulnerabilities

30

Cross VM traffic

A further area of concern with virtualization has to do with the potential for undetected network attacks between VMs that are colocated on a physical server. The problem is that unless the traffic from each VM can be monitored, you cannot verify that traffic is not possible between VMs. There are several possible approaches here, the first is that the VM user can simply invoke OS-based traffic filtering or firewalling. One potential complication that can be faced by a customer who needs multiple communicating and cooperating VMs is that these VMs may be dynamically moved around by the service provider to load balance their cloud. If VM Internet Protocol (IP) addresses change during this relocation (unlikely, but possible between VM instantiations) and absolute addressing is used for firewall rules, then firewall filtering will fail.

Although a tenant or customer may have on-demand access to security controls such as virtual firewalls, authentication services, and security logging, these services may undergo change as the underlying implementation is patched or updated. Firewall rules and other security configuration data may become operationally incorrect as VM images are re-provisioned in an updated or reconfigured infrastructure.

Although this is typically handled by public cloud implementations, there is a need for fundamental improvement in areas such as version control and configuration management for cloud implementations.

There are other risks, including unintended interactions or information transfer when on-demand security controls are integrated with a customer application. Recycled user IDs and IP addresses also represent concern if recycling an IP or UID makes it possible for a user to inadvertently gain access to an information resource that is not theirs. The essential issue here has to do with the correctness and completeness of the process that implements allocation and deallocation of any VMs, information resources or enabling elements.

Cloud Data Storage

There are several concerns around cloud data storage, and these include the following:

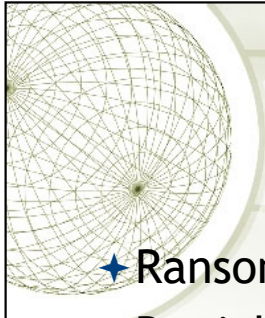
- 1) Since clouds tend to implement storage as centralized facilities, some view storage as having the potential to be an attractive target for criminals or hackers. This has always been the case for any valuable resource and can be mitigated by the application of appropriate security controls.
- 2) Multitenancy again presents concerns, this time with the potential for data isolation mechanisms that may either fail in operation or in a rollback operation from a backup system.
- 3) Storage systems are complex hardware and software implementations. There are always questions as to the potential for catastrophic failure modes that might either destroy the data or expose the data from one customer to another customer.

Loss of Physical Control Since tenants and users lose physical control over their data and applications, this results in a range of concerns:

- Privacy and Data With public or community clouds, data may not remain in the same system, raising multiple legal concerns.
- Control over Data User or organization data may be comingled in various ways with data belonging to others.
- A tenant administrator has limited control scope and accountability within a Public infrastructure-as-a-service (IaaS) implementation, and even less with a platform-as-a-service (PaaS) one. Tenants need confidence that the provider will offer appropriate control, while recognizing that tenants will simply need to adapt their expectations for how much control is reasonable

within these models.

New Risks, New Vulnerabilities There is some concern that cloud computing brings new classes of risks and vulnerabilities. Although we can postulate various hypothetical new risks, actual exploits will largely be a function of a provider's implementation. Although all software, hardware, and networking equipment are subject to unearthing of new vulnerabilities, by applying layered security and well-conceived operational processes, a cloud may be protected from common types of attack even if some of its components are inherently vulnerable.



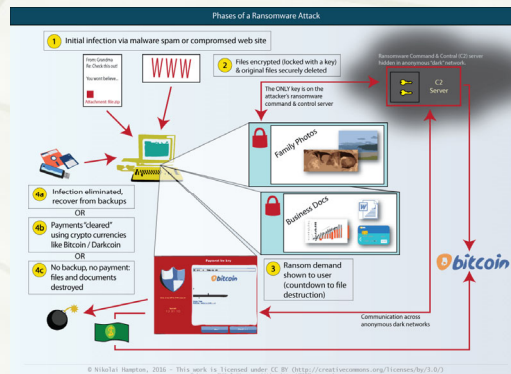
Common Attacks

- ✦ Ransomware attacks
- ✦ Denial of service/Distributed denial of service (DoS/DDoS) attacks
- ✦ Data exfiltration
- ✦ SQL Injection attacks
- ✦ Cross site scripting (XSS) attacks
- ✦ Phishing attacks
- ✦ Virus/malware

31

We look at common attacks to data and systems nowadays

Ransomware Attacks



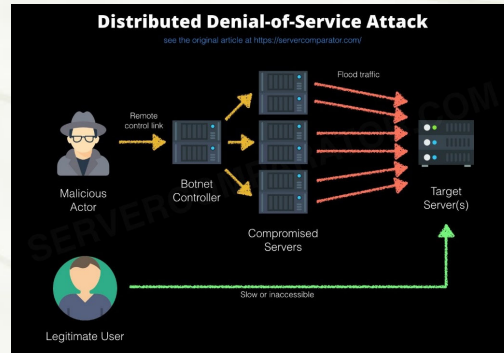
<https://www.weforum.org/agenda/2017/05/ransomware-what-is-it-how-does-it-work-and-can-you-protect-yourself>

32

Students are encouraged to do further reading from relevant articles, for example

<https://en.wikipedia.org/wiki/Ransomware>

Distributed Denial of service



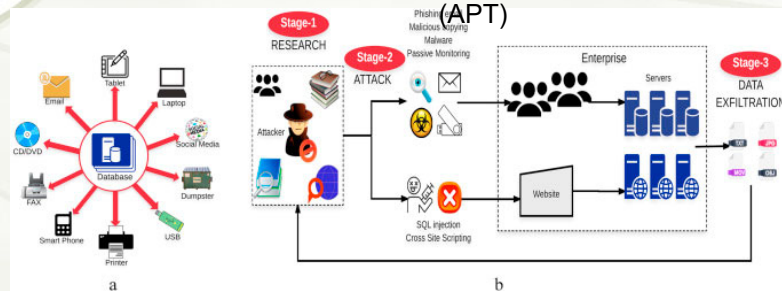
<https://blogs.msdn.microsoft.com/mlserver/2017/07/11/understanding-server-traffic-logs-and-detecting-denial-of-service-attacks/>

33

Reading <https://www.cloudflare.com/en-au/learning/ddos/what-is-a-ddos-attack/>

Data Exfiltration

a.k.a. advanced persistent threat
(APT)



<https://www.sciencedirect.com/science/article/pii/S1084804517303569>

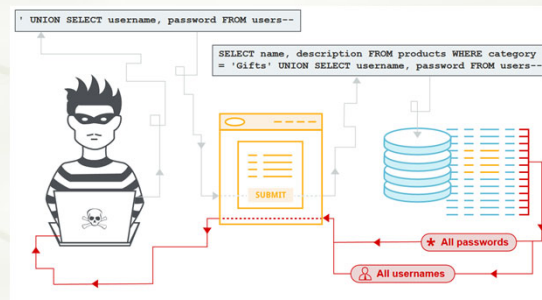
34

Some useful references

<https://resources.infosecinstitute.com/anatomy-of-an-apt-attack-step-by-step-approach/#gref>

<https://azeria-labs.com/data-exfiltration/>

SQL Injection



<https://portswigger.net/web-security/sql-injection>

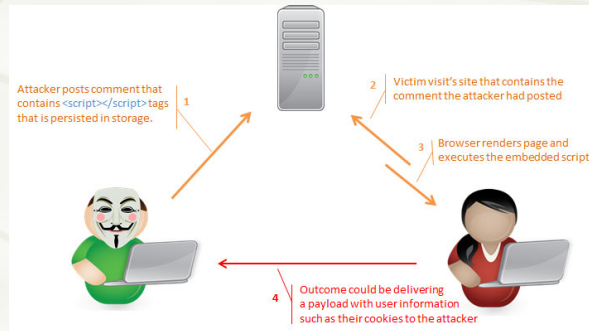
35

Reading

https://en.wikipedia.org/wiki/SQL_injection

<https://portswigger.net/web-security/sql-injection>

Cross-site Scripting (XSS)



<https://blog.sucuri.net/2016/04/what-is-an-xss-vulnerability.html>

Phishing



<https://madhatmedia.com.au/linkedin-spear-phishing-attacks/>

37

Reading

<https://en.wikipedia.org/wiki/Phishing>

<https://www.imperva.com/learn/application-security/phishing-attack-scam/>

Virus/malware



<https://uk.norton.com/internetsecurity-malware.html>

38

Reading

<https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html>



Need to Know

- ★ Generally how attacks happen
- ★ What issue: Availability, Integrity, or Confidentiality?
- ★ How to address the threat?
 - ◆ Prevention
 - ◆ Detection
 - ◆ Correction
 - ◆ Recovery

39