Chapter 5

Thursday, August 10, 2023 10:55 AM

Summarize virtualization concepts

Virtualization - popular tech in data centers

host 1 or more virtual systems, machine, on single physical system

hypervisor - the software that creates, runs, and manages VMs

VMware, Microsoft hyper-V, oracle VM

host - physical system hosting VMs

even though it requires lots of resources, still less expensive than multiple systems

guest - OS running on host system

most hypervisors support multiple OS and 32- or 64 bit

host scalability - ability to resize computing capacity of VM

more mem, processors, disk space

more mem, processors, disk space

host elasticity - dynamically change resources assigned to VM based on load

Virtualization has best ROI when org has lots of unused servers

if there are lots of servers that all have high usage, convert to VM would reduce electricity or heating but might not reduce total cost of ownership

Thin clients and virtual desktop infrastructure

thin client - pc w/ enough resources to boot and connect to server to run specific apps or desktops

virtual desktop infrastructure **VDI** - hosts users desktop OS on a server

typically access within network to connect

typically access within
but also possible to connect
from phone

Containers

Container virtualization - runs services or appr within isolated containers or app cells

host's OS and kernel run service or app within each container

services/apps in one container can't interfere w/ others

uses fewer resources than traditional type II hypervisor virtualization

one con is that all containers must use host OS

VM Escape Protection

VM escape - attack that allows attacker to access host system

VM escape

attacker to access host system from within VM

host system runs an app or process called hypervisor to manage VMs

many hosts have elevated privileges attacker would likely get access to all VM in host

need to patch physical and virtual servers

VM Sprawl Avoidance

VM sprawl - have many VMs that aren't properly managed

Change management process

bad for resource usage too

Replication

VM are just a group of files

VMs are just a group of files

easy to copy a VM from one server to another

Snapshots

Snapshot - copy of a VM at a moment in time

before updates, tests, new controls...

Non-Persistance

persistant virtual desktop - each user has a custom desktop image

can customize and save files but at the cost of many resources disk space

non-persistance - same desktop for all users

reverts to last snapshot after log off

live media USB bootable drives - changes to OS on drive

live media USB boot

save any changes to OS on drive

Implementing Secure Systems

ensure that systems are deployed and maintained in secure state

Endpoint security

endpoint detection and response EDR

or endpoint threat detection... ETDR

provides continuous monitoring of endpoints

provide protection from threats that get through tools like IPS/IPS

deep dive in all activity on endpoint

commonly include

- anti-malware
- HIDS
- app allow/block lists

Hardening Systems

Hardening Systems

Hardening helps eliminate vulns from default configs, misconfigs, weak configs

Systems should only have apps, services, and protocols they need to meet their purpose

Uninstall unneeded software

modify Registry so powershell activity is logged, normally it bypasses logs

disk encryption

use vulnerability scanners to discover vulns

Configuration Management

Configuration management - help orgs deploy systems with secure configs

baselines + imaging

use naming conventions for version control

PC_Sales_3.0

Secure Baseline and Integrity Measurements

1. Initial baseline config
2. Integrity measurements for baseline deviation

auto tools monitor for changes

vuln scanners monitor and report

group policy auto reconfig systems if changes spotted

3. Remediation

NAC methods that quarantine systems

Using Master Images for Baseline Config

image - snapshot of single system that admins deploy to multiple

trust admins of
other systems

capture and deploy image

1. Start w/ blank source system
   install OS, apps, and configure

2. Capture image
   becomes master image
   image is file to be saved

3. Deploy image to multiple systems

secure starting point
   image contains all configs
   verified to be secure

reduced costs
   support doesn't need to learn
   tons of end user env

not just for desktops; for servers

not just

as well

Patch Management

patch management - ensures systems are up to date with current patches

smaller orgs could do auto

often test updates in sand box

VM

deploy using

Microsoft Endpoint Configuration

system management tools also include verification that verifies patch deployment

could combine w/ NAC to quarantine

Change Management Policy

change management - process for any type of system mods or upgrades

type of system mode or IP

- ensure changes to sys don't result in unintended outages
- accounting structure for all changes

Application Approved Lists and Block Lists

approved lists and block lists are both endpoint security solutions

authorized apps to run or apps to block

allow lists blocks everything not in the list

block lists allow everything not in the list

Mobile device management MDM systems use these lists

can quarantine apps so they can't run on system but is retained to examine it later

to examine

Application Programming Interfaces

API - software component that gives developers access to features or data in another App

common considerations

- Authentication - auth to keep unauth entities from using API
- Authorization - diff levels of access depending on user, service, etc.
- transport level security needs strong security like TLS when transferring data

API inspection and integration - testing API for security and usability

Microservices and APIs

Microservices - code modules designed to do one thing well

...ch service APIs are unique to each

web service APIs are unique to provider

a microservice could be used for many providers

FDE and SED

full disk encryption **FDE** - encrypts an entire disk

VeraCrypt

self encrypting drives **SED**

aka **hardware-based FDE drives**

encryption built into drive

users enter creds to decrypt drive

Opal storage specification - set of specs for SEDs

defines what vendors need to do to ensure SEDs are configed to prevent unauth access

opal-compliant - requires uname/pwd to unlock drive

to unlock

Boot integrity

verify integrity of OS and boot loading systems

ex: verify key OS files aren't modified

measured boot - goes through enough of the boot process to perform these checks w/out allowing users to access system

won't boot if system fails checks

Boot security and UEFI

Basic Input/output system **BIOS**

includes software that provides pc w/ basic instructions on starting

runs basic checks, locates OS, and boots

hardware chip that has software

firmware

Newer systems use **Unified extensible**

newer systems use Unified Extensible Firmware Interface UEFI
does many of same things but
- w/ enhancements
boot from larger disks
designed to be CPU-independant
upgraded through flashing - overwrites
software within the chip

Trusted Platform Module

TPM - hardware chip on motherboard
that stores crypto keys
provides full disk encryption
locks hard drives believed to
verify and auth process
supports boot attestation - captures
sigs of key files used to boot
and stores report
when sys boots w/ secure boot it
- boot files w/ stored sigs

when sys boo
compares boot files w/ stored

remote attestation - like secure boot but doesn't check TPM stored report, checks remote system stored report

TPM ships w/ unique RSA private key matched w/ public key to provide hardware root of trust or a known secure starting point

TPM can also store/generate other keys for decrypting disks

use an app like BitLocker to enable TPM

Hardware Security Module

HSM - security device can add to sys to manage, generate, and store crypto keys

High performance - external net apps using TCP/IP

- Using (cut)

Smaller - expansion cards you install in a server or as devices you plug into PC ports

microSD HSM - microSD card that includes HSM

Supports TPM security methods

HSM is removable device unlike TPM

can add HSM at any time

Protecting Data

Security policy - helps classify and label data

Data Loss Prevention

DLP - methods like blocking use of removable media and watch outgoing data or unauth data transfers

configure to look for specific strings

configure

Rights Management

rights management or digital rights management refers to tech to provide copyright protection for copyrighted works

Removable Media

USB data blocker - prevents software from writing any data to USB some will also prevent reading

orgs often prohibit flash drives

Data Exfiltration

data exfiltration - unauthorized transfer of data outside the org

DLP can scan any emails, files attached, and even zip files

ex: DLP could contain mask for SSN

can scan email, FTP, HTTP

exfiltrated

can scan email, ...

data often encrypted before exfiltrated so it can look for encrypted data for alert

Protecting Confidentiality with Encryption

authentication access controls only work so much

attackers can steal laptop and remove drive to take ownership of files

encrypted data is much harder to get

Database security

possible to encrypt entire db but more common to encrypt specific data

pwords can be hashed and salted

tokenization - replace sensitive data w/ sub values

Summarizing Cloud Concepts

Summarizing Cloud Concepts

Software as a Service

SaaS - any software or app provided to users over a network like the internet

typically browser-based

Platform as a Service

PaaS - pre-configed pc for customers to use as needed

easy to config OS and appropriate apps

managed hardware solution

you manage installed software but OS and other infra for server itself is managed by CSP

Infrastructure as a Service

IaaS - allows org to outsource its equipment

CSP owns equipment and maintains hardware

self-managed

users manage OS and all apps patches as well

serverless architecture - orgs build and run apps w/out managing infra

Anything as a Service

XaaS - everything not in SaaS, PaaS, IaaS comms, db, desktops, storage, security

IT as a service

Cloud Deployment Models

identify who has access to cloud infra

public cloud - provide to anyone from 3rd party companies sometimes buy them

private cloud - setup for specific orgs org hosts own servers and make servers available to employees via

internet

community cloud - companies w/ shared concerns can share resources

hybrid cloud - combo of any of these

Managed security service Provider

managed security service provider MSSP

3rd party vendor that provides sec services for smaller orgs

MSSP can provide

- Patch management
- Vuln scanning
- Spam and ims filtering
- DLP
- VPN connections
- Proxy services
- IDS / IPS
- UTM
- NGFW

MSP - Same

Managed service provider MSP - same but for all IT services

Cloud Service Provider Responsibilities

middleware - software added to OS to extend basic capabilities

ex: Apache for Linux as a web server

runtime - hosting env such as container on a server

isolates each customer's env from others

Cloud security controls

... and high availability

Cloud security

high availability and high availability across zones

no downtime

using multiple load balancing nodes that are in different places

resource policies

customers rent resources and don't rent more than they are allowed

secrets management

pwords / encryption keys

integration and auditing

integrate security controls into resource w/ ways to audit them by customers

Cloud-storage

- permissions - who can access data
- encryption
- replication - copy data and store somewhere else

- replication - copy data somewhere else

Cloud-based networks

- virtual networks
  typically use SDN tools rather than physical switches, routers
  can be hosted by 1 server
- public and private subnets
- segmentation
  segment pcs or networks just like local nets w/ VLAN and screened subnet
- security groups
  role-based etc
- dynamic resource allocation
  elasticity
- instance awareness
  know how many instances of resources an org is using

resources are [illegible]

- **Virtual private cloud** **VPC endpoint**
  VPC endpoint is virtual device within virtual network
  connect to endpoint then access resources to save bandwidth

- **transit gateway**
  connect VPCs to on premise network

- **container security**

On-premises versus off-premises

on-premises - all resources owned, operated, and maintained in org's property

off-premises - rent from CSP

Cloud Access security Broker

CASB - software tool or service deployed between org's net and cloud provider
monitor traffic and enforce policies

on-premise = all endpoints need
[illegible] installed

on-premise = all endp
to have installed

off-premise = all traffic redirected
to CASB

Cloud-based DLP

protect cloud data by doing things
like detecting PII

Next Generation secure web gateway

SWG - combo of proxy server and
stateless firewall

clients are configured to access all
resources through SWG

- URL filtering
- malware detection
- packet filtering
- Network DLP
- Sandboxing

Firewall considerations

common to use 2 firewalls to make
a screened subnet

common to use
screened subnet
just like non-cloud

cloud firewalls operate on all layers of OSI

small orgs can run firewall

large orgs can run servers to act as firewall

Infrastructure as Code

managing and provisioning data centers with code to define VMs and virtual networks

admins can use scripts to create virtual objects

Software-Defined Networking

SDN - uses virtualization techniques to route traffic instead of switches/routers

Separates

data plane - forward/block traffic

control plane - identify path to take

data plane was always based on routers and ACL, SDN doesn't

routing protocols like first OSPF and protocol BGP - determine best path to route traffic on control plane

implements ABAC

Software-defined visibility SDV

SDV - tech used to view all net traffic

Edge and Fog computing

edge computing - storing and processing data close to the devices that generate and use data

fog computing - same but uses a net close

fog computing - same but uses a ...
to device w/ multiple nodes
edge only uses 1 node

Cloud security Alliance

CSA - non-profit that promotes cloud best practices

Cloud Controls Matrix CCM - cybersecurity control framework

Deploying Mobile Devices securely

mobile devices need attr like OS, OPS, network interface, ...

Deployment Models

corporate-owned

org purchases and issues devices

COPE Corporate owned, personally enabled

employees are free to use device as ... then owned it

employees as if they owned it

BYOD bring your own device

can have any possible device and connect to network

CYOD choose your own device

list of acceptable devices

Connection Methods and Receivers

cellular

3G, long-term evolution LTE, 4G, 4GLTE, 5G

wifi

almost always have wireless network interface

bluetooth

NFC

typically for payment

RFID

Some NFC systems use RFID

Infrared

line-of-sight wireless tech

usually for tv remotes

apps for phones to be universal remote

also possible to use for file transfer

USB

point to point

connection between two wireless devices

can be bluetooth, RFID, NFC

point to multipoint

creates an ad-hoc network

wireless devices connect to each other w/out AP

ad hoc vs infrastructure mode (AP)

Ad hoc vs infrastructure

payment methods

might restrict payment on COPE devices

Mobile Device Management

MDM - tech to manage mobile devices

Some vendors sell unified endpoint management UEM solutions to manage mobile devices

make sure they are updated

antivirus

Microsoft endpoint configuration Manager

MDM concepts

- Application Management

restrict what apps can run

mobile application management MAM

mobile application management MAM

- Full device encryption

  not always possible w/ employee owned

- Storage segmentation

  isolate data

  may require to use external storage for corp data

  encrypt certain segments

- Content management

  ensure that appropriate content is stored in segments

  enforce auth when accessing certain data

- containerization

  can implement containers in mobile devices to encrypt what

  entire device

mobile device

encrypting entire device

can run org's app in container

- passwords & PINs
- Biometrics
- screen lock
  lock/unlock w/ pin
- remote wipe
  remote signal to wipe/erase all data
- geolocation
  GPS
- geofencing
  virtual fence or boundary
  ex: org apps only run inside fence

- GPS tagging

  geotagging

  add geo info to files like pictures

- context-aware authentication

  use multiple elements to auth a user and device

- push notifications

Mobile Device Enforcement and Monitoring

org owned = MDM downloads/installs required updates

emp owned = MDM monitors and blocks non-updated devices

Unauthorized software

typically ban apps from 3rd party app stores

jailbreaking

rooting - modify android to get

rooting - modify android ... to root-level access

mobile typically stores OS in onboard memory

flash memory - retain data when not powered

OS = software
+ mem = hardware
firmware

updates to OS overwrite firmware
using over-the-air OTA updates
firmware OTA updates

possible to overwrite w/ custom firmware
other option to rooting

sideloading - copying app package in app packet kit APK

stat... J

in app packet kit APP

good for devs testing apps but dangerous when downloading 3rd party

Messaging services

Short message service SMS and multimedia Messaging service MMS

SMS = basic text

MMS = + images...

both send text in plaintext

attackers can send MMS to gain remote code execution privileges

rich communication services RCS

newer comm proto to replace SMS

+multimedia

Hardware control

MDM can block camera/mic
might not be able to block based on geofence

Universal serial bus or type c **USB OTG**
connect almost any devices
MDM can prevent external media

Unauthorized Connections

tethering - share device's internet connection w/ another
used within org can bypass firewalls/proxy

hotspots - allow multiple people to share internet
can bypass network controls like tethering

Wi Fi Direct - allows devices to connect w/out wireless AP or router

w/out wireless

like wireless ad-hoc network

single radio hop comms - none of devices can share internet

ad hoc can share using multihop wireless comms

subscriber identification module SIM

id's countries/ networks phone will use

carrier unlocking

may be blocked in COPE

SE android

security enhanced android

uses security-enhanced Linux for access security

default denial - anything not in SELinux policy is denied

SELinux

enforcing mode - enforces SELinux policy

permissive mode - does not enforce but logs all activity that would be blocked

Exploring Embedded Systems

embedded system - any device that performs specific function and uses pc to perform function

ex: wireless multifunction printer includes embedded system

Security+ embedded systems

- field programmable gate array FPGA
  programmable integrated circuit IC
  installed on circuit board

transfers config program from config memory chip

transistors
memory chip

can remember programming and also be rewritten

- arduino - microcontroller board
  contains CPU, RAM, ROM
  no OS but uses firmware
  for simple tasks like monitor temp in LCD screen

- raspberry pi - microprocessor-based
  mini-pc
  raspberry Pi OS
  ex: can monitor temp and send signals to HVAC

Understanding IoT

commonly use embedded systems and connect to central device to comm via internet, bluetooth, etc.

comm via internet / ...

industrial control systems ICS - broad term encompassing SCADA systems, distributed control systems, and prog logic control PLC systems

ICS and SCADA Systems

industrial control sysem ICS - systems in large facilities

SCADA typically controls ICS by monitoring and sending it commands

typically in isolated netr that cant access internet

Common uses

- manufacturing & industrial
- facilities
- energy

- logistics
  shipping facilities

some are in corpo net
but typically in isolated VLAN

Iot and Embedded systems

- smart TV
- wearables
  fitbit
  microchips
- wireless thermostats, lighting, coffee
- camera systems
- system on a chip SoC - integrated circuit that includes all functions of computing system
  typically has app inside onboard mem
- real time OS RTOS - os that reacts to input within specific time

to input within [illegible]

ex: assembly line

raises error if no input given within set time

Security Implications of embedded systems

big challenge is keeping embedded sys updated

vendors are not fast at putting out patches

default config also need to be assessed

Embedded System Constraints

compute

small, no full CPU, ...

crypto

too small to use all crypto proto

power

[illegible] power supplies, use

power

dont have own power supplies, use parent's

range

low range

authentication

often dont have

network

might not have interface to connect to net

cost

expensive to add security to device

inability to patch

often not possible to patch

implied trust

most people trust they are secure but not true case

most pop-
but not true case

weak defaults

Communication considerations

5G
better speeds than 4G

limited range
1000 ft vs 4G 1 mile

can be blocked physically

narrow-band
very narrow frequency range

two-way radio systems
(walkie talkies)

Baseband radio
include frequencies very near 0

used when transferring data
over cable

SIM cards

used to connect to provider

region-based

Zigbee - suite of comms proto for smaller networks like in a home

has higher sec but lower capabilities

Assessment Notes

1. Check server and clim any weak configs

disable unused services

2. Best method to test updates

sandbox

3. Malicious traffic; may be malware

compare to lists from master image

and it must be problem

and it must

integrity measurements

4. Best way to prevent RAT install

allow list

5. Encrypt drive w/out user interaction

SED

6. Secure boot that checks remote configs

Remote attestation

7. Reduce data exfil using external storage devices

block write capabilities to removable media

DLP would not stop this

network DLP would not stop

8. PaaS = CSP provides hardware/software

9. IaaS = servers, storage, net, but nothing else

10. CASB = service between org net and CSP for sec

11. Next-gen SWG = URL filter, DLP, malware filter for web

12. MDM = comprehensive solution to protect org data in BYOD

13. MDM application can assign unique ID to devices to manage remotely

14. Containerization best for BYOD

15. Jailbreaking can download

15. Jailbreaking can -
3rd party apps