CISSP® CBK® MAY 2021 UPDATE
NEW TOPICS STUDY GUIDE

This document focus is the new content added to the CBK® as of May 1st, 2021.

This guide is from
Clement Dupuis, CD
Owner and Founder of CCCure

A WARM WELCOME FROM CLEMENT

Good day to all, this is Clement, the owner and founder of CCCure.

I would like to welcome you to my new **CISSP CBK May 2021 study guide.** I have built it to help you make sense, study for, and get ready for your exam without the need to invest in more resources to cover the new topics of the May 2021 CBK.

The new exam based on this CBK Update will be coming into effect on the 1st of May 2021.

Please feel free to share it with your friends and colleagues. All I ask is that you do not modify it and you leave the document as is as per the Creative Common license that I am using for it.

The new UPDATE from (ISC)², and I must stress the keyword UPDATE, is not a new CBK or a totally new version of the exam. As it has been the case with previous updates, the number of changes is minimal, mostly cosmetics, and a whole lot of renumbering of topics. You certainly **DO NOT** need to buy new books, take more training, or start your studies from zero again. Even thou some of the training companies and book authors would like you to believe otherwise.

(ISC)², talks about this in their Update FAQ as it is a frequently asked question, they state:

===== Beginning of extract from the (ISC)² Update FAQ =====

Q: **If I have been studying for the CISSP® exam with material that focuses on the current domains, will I be sufficiently prepared to take the new exam without additional study?**

A: (ISC)² exams are experience-based that include experience-based items that cannot be learned by studying alone. If you already have the experience in the domains covered in CISSP® and believe that you have sufficiently studied those domains, you should feel confident that you are qualified to take the new exam and pass it. (ISC)² cannot guarantee you will pass the exam.

======== End of Extract from the (ISC)² Update FAQ ========

We will see what they are, how they apply, and allow you to learn what you may not have learned yet from the current study resources that you have, this way you can complete your studies without missing any important topics that you must know.

Overall, I was quite pleased with this update to the CBK®, finally (ISC)² added more details to some of the very high-level topics that did not make a lot of sense to most students. It would be like me saying: “For the problem you have at the moment, just eat a fruit”. That does not tell you much, it is too obscure. You expect me to tell you a lot more details such as what is the fruit you must use? What quantity? In what way? (cooked, raw, mix with something, etc.…). It was refreshing to see more details added to the topics of the CBK®, the content should not be a secret.

WHY IS THERE SO LITTLE CHANGES TO THE CBK®?

This is one of the most common questions that I get. Overall, I would say there is only 2% of new material that was added to the May 2021 CBK® and I am being generous here.

The CBK® is based on CONCEPTS, in fact, multiple hundreds of them. Those concepts do not tend to change much over time. Concepts like Integrity, Confidentiality, Availability, Authentication, Authorization, Accounting, and the list could go on and on. Concepts do not change but the tools and techniques used will change greatly over time.

Therefore, the content tends to be static over the year with a bit of new content added every 3 years or so.

WHEN WILL (ISC)² OFFER ONLINE EXAMS LIKE OTHER CERTIFICATION BODIES

You probably heard through the grapevines that (ISC)² has recently conducted a study about the feasibility and challenges of conducting online remote exams while protecting the integrity of the exam as well. The results of their study have not been released yet and we do not know if online exam from a remote location will be available in the future. We are keeping a close watch and will let you know if we find more details.

COMMENTS – ADDITION – ERRATA – FEEDBACK

We welcome all comments, and this is how we can further improve this study guide. You will not offend us; we are human being and we could inadvertently make an error or a typo.

If you have found a typo, an error, or omissions that you would like to add to the guide. Please, do let us know by sending an email to clement.dupuis@cccure.com with the subject line **FEEDBACK NEW TOPICS STUDY GUIDE 2021**, and we will get it fixed immediately and give you the proper credit for your contribution.

$$$ EXAM PRICING $$$

As of the 1st of May 2021, you will need to fork a few more dollars to take the exam. The CISSP® exam registration fee will increase from U.S. $699 to U.S. $749 on the 1st of May.

WHAT ABOUT ANNUAL MAINTENANCE FEES (AMF)?

Those were raised at the beginning of 2019. They were raised from $85 USD to a nice $125 USD. That was quite a steep increase in pricing. We are talking about 47% percent as an increase. So, I do not expect them to be raised again this year, but it is up to (ISC)² to decide and not me.

There is a nice article written by Wim Remes, who used to be a board member from 2012 until 2014 and from 2016 until 2018. The articles shed some light on the fees and what they are used for but also highlight some of the shortcoming and improvements that could be done.

https://www.linkedin.com/pulse/isc2-fees-price-being-professional-wim-remes/?published=t

The article mentions there was 140.000 members as of January 2019, the revenue from AMFs was close to $12 million or about 20% of total revenue of (ISC)². That many members at the current AMF fees would be 17 Million in revenue using the number of members from 2019, today I am sure there is a lot more members today, it usually increased quite a bit every year.

I wish everyone all the best in their studies.

Feel free to link with me on LinkedIn at https://www.linkedin.com/in/clementdupuis/

The best way to contact me is through email at clement.dupuis@cccure.com I get multiple hundreds of emails daily, please use a good subject line such as “CISSP CBK 2021 STUDY GUIDE” and I will give priority to your email.

Best regards

Clement

LIMIT OF LIABILITY / DISCLAIMER OF WARRANTY

I wish to make clear this document is not provided by (ISC)² or endorsed by (ISC)² and does not make any such claim. It is best used as a complement to The Official (ISC)2 Guide to the CISSP CBK Reference which is the official study book produce by (ISC)².

The author makes no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose.

No warranty may be created or extended by sales or promotional materials. The information, advice, and strategies contained herein may not be suitable for every single student or situation. This work is provided with the understanding that the author is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought.

The author shall NOT be liable for damages arising here from. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author endorses the information the organization or Web site may provide or recommendations it may make.

Any logo, brands, or trademark mentioned or used within this document is the property of their respective own.

Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read. Let us know so we can update the links.

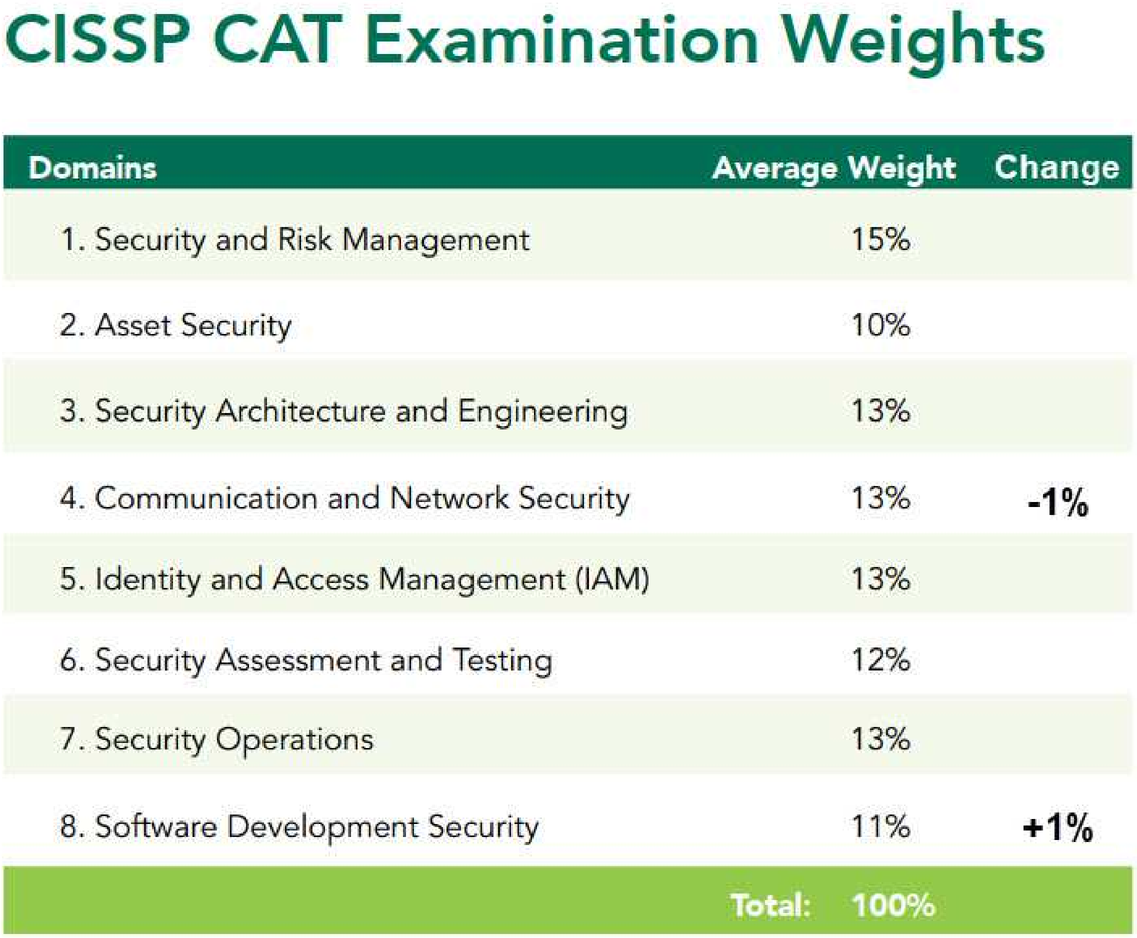
This study guide is provided to you "AS IS". It is distributed under the following license:

DOMAIN WEIGHTING

As you can see in the graphic below. The weighting of each of the domains within the new CBK® has not changed much. Domain 4 went down by 1% and Domain 8 went up by 1%.

Considering the adaptive exam is 100 to 150 questions, this means you may get a few questions less in domain 4 and few more questions in domain 8 when you take the exam. So, no worries at all, same old same old but in different domain within the CBK®.

The same percentage applies if you do the linear exam in a language other than English. Other languages (French, German, Brazilian Portuguese, Spanish, Japanese, Simplified Chinese and Korean) are delivered the old way where you have 250 questions and six hours to complete the exam.



CISSP CAT Examination Weights

Domains	Average Weight	Change
1. Security and Risk Management	15%	
2. Asset Security	10%	
3. Security Architecture and Engineering	13%	
4. Communication and Network Security	13%	-1%
5. Identity and Access Management (IAM)	13%	
6. Security Assessment and Testing	12%	
7. Security Operations	13%	
8. Software Development Security	11%	+1%
Total:	100%	

The graphic above was extracted from the (ISC)² CBK® available at: https://www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/CISSP-Exam-Outline-English-April-2021.ashx?la=en&hash=FE6EAF9902ADABBD2E733164E93E5CB24B9C08F0

THE CCCURE QUIZ ENGINE at https://cccure.education

This study guide will be a great supplement to your studies by filling the gaps on topics that may not be within any of the study resources you have for your CISSP studies.

Many students have reached out to me and ask me: "Clement how do I know if I am ready for the exam and I have retained the key topics that I must know within all of the 8 domains of the exam?"

I always recommend to them to subscribe to my Quiz Engine located at https://cccure.education The quiz engine is currently being updated with questions to cover 100% of the topics of the May update.

If you score consistently above 80% on each of the domains of the quiz engine, you are ready for the real exam.

The quiz engine has been up and running for over than 23 years. More than 250,000 students have used it to prepare for their exam and pass on the first trial. It is the same quiz engine that I use within my live and online classes that I teach. The engine has a lot of features and most of those features were requested by students like you, see below a partial list of available features:

- Our subscriptions are very affordable to anyone studying.
- The engine has more than 2000 questions covering all the key topics of the CBK.
- The exam will fill the gap with topics you may not have seen in any study resource. Some of the topics are concepts you are expected to know based on your 5 years of experience.
- We offer multiple choices, scenario-based questions, drag and drop, and Hotspot.
- All questions have thorough explanation of the correct choices and the incorrect ones as well.
- Your subscription gives you access to all the certifications we support and not only one.
- The quiz engine offer STUDY MODE and TEST MODE. In study mode you can see the answer right away as you take the quiz, this is great for learning. In TEST MODE you simulate the real exam where you see the question only once, you must answer it and then move to the next.
- You can do quizzes of 10, 15, 20, 25, 50, 75, 00, 125, 200, and 250 question.
- You can do quizzes on one domain, two or more domains, or all of them.
- You can do as many quizzes as you wish.
- The quiz engine will track your progress and allow you to review any of the quiz you have taken later if you desire.

- The quiz engine allows you to drill down on topics you have missed within previous quizzes. This is how you will work on your weak points and what YOU DON'T KNOW.
- The choices presented are shuffled so you do not remember the position, you remember the topic and its content instead. Which is what you need for the real exam.
- Exams are being timed using the same amount of time as the real exam. You can disable the timer at the beginning of your studies if you so desire. It allows you to review your note and learn as you take quizzes.
- The engine is constantly updated with the latest tips and content, it is not a static exam.

If you made it this far, I have a special rebate code for you, the rebate code is: **CLEMENT**

Apply the code at checkout time to get an instant **15%** OFF

Contents

ARTIFACTS (e.g., Computer, Network, Mobile Device) (Related to Forensics)

Cell phones, computers, mobile devices, servers, surveillance systems and other digital devices are repositories of CONTENT. Content includes user documents we are all familiar with such as: Word files, spreadsheets, emails, instant messaging, text messages, etc.

While it is true you can garner a lot of information from content – there is a whole other world of information that exists that you may be missing: ARTIFACTS. Digital artifacts are not only more interesting but most importantly can provide far more validity to proof or factual evidence.

So, what is an artifact in cyber security? Artifacts are tracks that get left behind. You could associate them with the footprints of the end-user or hacker. However, end-users are often unaware that artifacts exist. Like permanent footprints, they are challenging to manipulate. As a result, artifacts help cyber security consultants in their role of uncovering the root causes of a data breach and the threat actors involved. As a result, there is significantly more validity of proof by considering the artifacts.

The Locard's Exchange Principle

One of the foremost axioms of forensics, digital or otherwise, is Locard's Exchange Principle. Simply put, this principle, formulated by Dr. Edmond Locard (known in his time as "the Sherlock Holmes of France") states:

"Every contact leaves a trace."

These traces are the tiny pieces left behind that we forensic investigators use to help determine in each situation *what* happened, *where* it happened, *who* it happened to, *when* it happened, and *how* it happened, and who did it.

How Digital Artifacts Are Used

1. Artifacts are used to corroborate the information in the content.
2. Artifacts can reveal things that content never will. (We've yet to find a case where somebody wrote a document (content) where they said, "Dear Boss, this is the stuff I'm going to steal from the organization today." Yet – working from the artifacts Digital Forensic Experts can tell just that.
3. Artifacts can show intent or the state-of-mind of the individual. This includes what internet searches were being conducted and what web pages were visited or researched as an example.

Examples of digital artifacts garnered from web searches:

- "Wife+Murder+Electrocution"
- "How to frame your employer for more severance pay"

- “When is the best time to start a fire”
- “How to cover your tracks in arson”

Artifacts are not readily available for an end-user to look at. You need to engage a Digital Forensics Expert.

Digital Forensics and Cyber Security Experts have both the tools and the knowledge to:

- Preserve the device so as not to trample (contaminate) on valuable artifacts;
- Know where to look;
- Accurately interpret the findings;
- Understand the subtle nuances as artifacts can mean different things depending on the Operation System (OS) and even the versions of software.

Sources:

- https://www.ssi-net.com/what-is-an-artifact-in-cyber-security/
- https://www.tetradefense.com/digital-forensics-services/what-are-forensic-artifacts-my-favorite-artifacts-part-0/

NOTE FROM CLEMENT:

The official book mostly covers the word artifact in the context of software development. Which is NOT what this addition is. This one is within the field of Forensics which is quite different.

BREACH & ATTACK SIMULATIONS

Here is an interesting tool that is up and coming. It will develop greatly in the next few years. See below information gathered from a Gartner posting on the topic:

Cyberattacks have evolved dramatically in the past couple of decades regarding their capabilities, scope, fallout, number of targets, etc. The worldwide damages from cybercrime are reaching all-time highs and it looks that this will only get worse. Since the risk of being attacked is so high, C-level managers and executives are looking to boost their organization's security posture. CIOs and CISOs are now pressured to prioritize cybersecurity and shift budget to acquiring additional security solutions making sure that they are resilient to cyberattacks.

Since testing the cybersecurity posture of organizations is becoming a top priority, it triggered an increased demand for the latest and most comprehensive testing solutions. Traditional ways of testing include scanning for vulnerabilities (which entails checking for vulnerabilities that are already known or that have already been exploited by cybercriminals), manual penetration testing (consisting of pen tests that are conducted by human testers who try to evaluate the security of an organization's infrastructure by safely exploiting vulnerabilities), and Red Team testing (where a Red Team consisting of cybersecurity pros attacks the organization's network, and a Blue Team consisting of IT managers and/or cybersecurity staff will try to stop these attacks).

In its Hype Cycle for Threat-Facing Technologies 2017, Gartner introduced a new domain: The Breach & Attack Simulation (BAS). Gartner defines Breach & attack Simulation (BAS) technologies as **tools "*that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means*"**. What makes BAS special, is its ability to provide **continuous and consistent testing at limited risk** and that it can be used to alert IT and business stakeholders about existing gaps in the security posture or validate that security infrastructure, configuration settings and detection/prevention technologies are operating as intended. BAS can also assist in validating if security operations and the SOC staff can detect specific attacks when used as a complement to red team or penetration testing exercises.

In its Hype Cycle for Threat-Facing Technologies 2018, Gartner rated the benefit of BAS as "**high**". **As an emerging technology**, it is expected to go mainstream within the next 10 years. Last year, Gartner predicted that it would take more than 10 years, which underpins the acceleration of BAS as becoming a mainstream technology and that the BAS market is proving the value and accuracy of security assessments resulting from simulated attacks. The installed base has approached hundreds of customers for leading BAS vendors in 2018. In its previous report, Gartner found that "*only a few vendors having real customer deployments*". It illustrates that CISOs are allocating budget for automated testing and assessment of existing security controls as well as the appropriate configuration settings for email and web security gateways, firewalls and web application firewalls, and ACLs.

Source: https://cyberstartupobservatory.com/breach-attack-simulation/

CLOUD ACCESS SECURITY BROKER (CASB)

A Cloud Access Security Broker (CASB) helps organizations extend on-premises controls or transform controls to the various cloud environments. A CASB does this by acting as a go-between, being a middleman between the cloud customer and the service provider.

Even when the cloud provider does not allow custom solutions for security, a CASB can augment security controls by monitoring for ingress and egress of data and services used in the cloud. A CASB is primarily a software solution that discovers unauthorized attempts at accessing private data. It can also use machine learning to watch human behavior on the network and alert security administrators when abnormal behavior happens, and a threat is suspected.

CASBs are not strictly only software. A CASB could be an external partner with people operating the service. In terms of visibility, CASBs provide the first measure of visibility into all the cloud applications being used by an organization, sometimes including unsanctioned use.

Regarding unsanctioned use or unauthorized abuse, access and authentication is the responsibility of the customer organization. To assist with that, CASBs may support account maintenance. CASBs help determine how cloud solutions and services align with the organization’s own established workflows. Sometimes an organization cannot overcome the challenge of merging internal processes with potentially useful cloud services. A CASB can, in that scenario, assist with enterprise integration.

CASBs can also provide functionality, such as data security and threat protection. In a manner like how SIEM systems use threat intelligence to provide alerting, the CASB draws upon numerous sources to evaluate URLs and services that users attempt to access to provide a risk assessment rating to security personnel.

Gartner defines it as:

Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 480-481). Wiley. Kindle Edition.

- https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs

CELLULAR NETWORKS (e.g., 4G, 5G)

NOTE FROM CLEMENT:
This was added to the CBK, but it was already covered in most of the books out there. I have included it as it is a new clarification that was added.

Cellular or mobile networks are wireless communications that traverse across cells. The cells are geographically dispersed areas that consist of one or more cell sites or base stations.

The cell site or base station is a transceiver fixed to a location. The user of a cell network uses a portable device over a specific set of radio wave frequencies to connect to the cell site and other cellular devices or the Internet.

The standard descriptors to differentiate cellular technology refer to the generation when the technology was introduced. This can be confusing. For instance, 1G and 2G mean first- and second-generation, respectively. It does not indicate a specific frequency or signal strength.

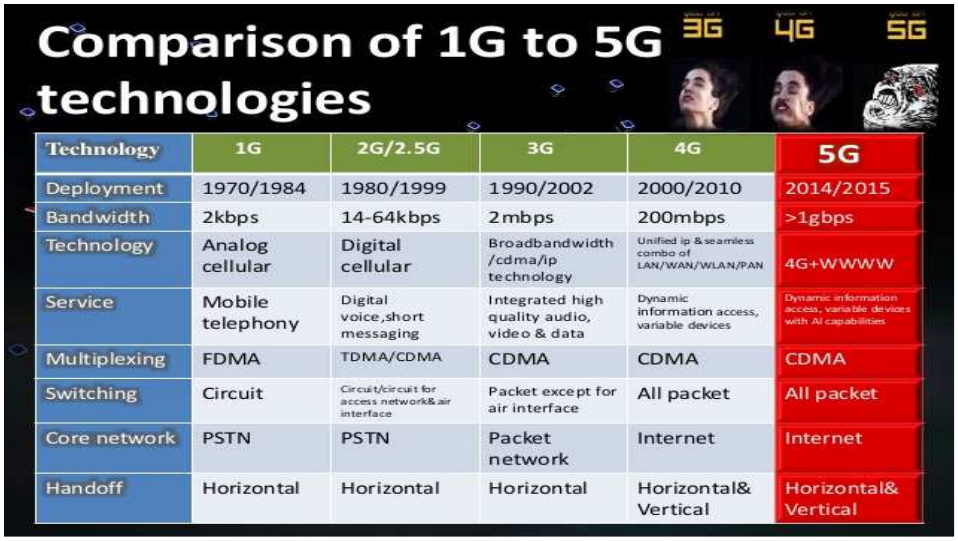
While many cellular technologies are labeled and sold as 4G, they may not actually reach the standards established for 4G by the International Telecommunications Union-Radio communications sector (ITU-R). The ITU-R set the standard for 4G in 2008. In 2010, the group decided that if a cellular carrier organization would be able to reach 4G-compliant services in the near future, the company could label the technology as 4G.

Standards for 5G have been in development since 2014. However, the 5G network and compatible devices are expected to be commercially available worldwide in 2020. There have been localized deployments, like at the 2018 winter Olympics in South Korea.

A security professional should keep some important considerations in mind when it comes to supporting and securing information sent and received in a cellular wireless network. Since 1G, cellular use is for much more than just voice. Cell phones today, i.e., smartphones, have higher-level computing power to run applications, transmit text, send images, stream video, and store significant amounts of sensitive data.

The Global System for Mobile Communications (GSM) standard has been developed and enhanced over time to support the use of text and data in addition to voice. For these reasons, communications that need to be secured will need additional technical controls in place.

Cellular transactions are not inherently secure. There are numerous tools available for attackers to intercept wireless transmissions. A common attack scenario uses cell base stations to conduct MitM traffic capture. These attacks can take place whether the cellular connections are to the Internet or just between two or more mobile devices.



Comparison of 1G to 5G technologies

Technology	1G	2G/2.5G	3G	4G	5G
Deployment	1970/1984	1980/1999	1990/2002	2000/2010	2014/2015
Bandwidth	2kbps	14-64kbps	2mbps	200mbps	>1gbps
Technology	Analog cellular	Digital cellular	Broadbandwidth /cdma/ip technology	Unified ip & seamless combo of LAN/WAN/WLAN/PAN	4G+WWWW
Service	Mobile telephony	Digital voice,short messaging	Integrated high quality audio, video & data	Dynamic information access, variable devices	Dynamic information access, variable devices with AI capabilities
Multiplexing	FDMA	TDMA/CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit/circuit for access network& air interface	Packet except for air interface	All packet	All packet
Core network	PSTN	PSTN	Packet network	Internet	Internet
Handoff	Horizontal	Horizontal	Horizontal	Horizontal& Vertical	Horizontal& Vertical

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 440-441). Wiley. Kindle Edition.

- You can get more info about 5G on the IEEE website at: https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g

COMPLIANCE CHECKS

Note from Clement: This is a subject that was added but it was already within the content of most study book and something being mentioned throughout those books as well. Now they have created a specific topic for it.

Cybersecurity Compliance involves meeting various controls (usually enacted by a regulatory authority, law, or industry group) to protect the confidentiality, integrity, and availability of data. Compliance requirements vary by industry and sector, but typically involve using an array of specific organizational processes and technologies to safeguard data. Controls come from a variety of sources including CIS, the NIST Cybersecurity Framework, and ISO 27001.

To begin working towards compliance, it is important to first figure out what regulations or laws you need to comply with. To start with, every state in the U.S. has data breach notification laws that require you to notify customers if their personal information is compromised. You can find the specific laws and requirements for your state here.

Compliance requirements vary vastly from state to state, and some apply regardless of whether your business is in the state. For instance, The California Consumer Privacy Act and the NYDFS Cybersecurity Regulation impose requirements that can apply to your business in any state if you deal with data pertaining to these acts. If your business deals with financial information of a resident of New York, for example, you would be subject to the set of requirements laid out by the NYDFS Cybersecurity Regulation regardless of which state your business is in.

Next, it is important to determine what type of data you are storing and processing, as well as which states, territories, and countries you are operating in. In many regulations, specific types of personal information are subject to additional controls. PII stands for Personally Identifiable Information, and includes any data that could uniquely identify an individual. Examples include:

- Social Security Numbers
- First/Last Name
- Date of Birth
- Address
- Mother’s Maiden Name

PHI stands for Personal Health Information and consists of any information which can be used to identify an individual or their medical treatment. Some examples of PHI include:

Medical Appointment Information, Medical History, Admissions Records, Prescription Records, Insurance Records

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 238). Wiley. Kindle Edition.
- For more details see the Cybersecurity Compliance Guide at:

  https://darkcubed.com/compliance

CONTAINERIZATION

This is a new term added to the CBK, however without any context it could mean a whole lot of thing. A quick search through the latest study book from (ISC)² (The Official (ISC)2 Guide to the CISSP CBK Reference), presents 3 instances of the term in different context.

1. In Browsers Security context:

   Browsers are adding sandbox or containerization features (e.g., Site Isolation in Chrome) that limit the ability of a website to affect other sessions or websites.

2. In the Bring Your Own Device (BYOD) Context:

   Application wrapping is the containerization of a third-party application to empower policies such as activity timeout or session timeout.

3. In the context of mobile device management and BYOD:

   BYOD has serious security implications for an organization. Security professionals will need to be able to implement specific security controls to accommodate the increasing popularity of BYOD as a method to control costs and improve employee productivity. Some general technologies to understand related to security are mobile device management (MDM), containerization, app virtualization, and secure containerization.

   To address many of these issues and to provide additional management and control over mobile devices, one can install MDM agents on mobile phones to provide additional security. These products provide a range of features, including:

- Jailbreak detection
- Vulnerability management (detection and possible resolution)
- Remote lock
- Remote wipe
- Device location
- Data encryption
- Sandboxing
- Anti-malware
- VPN
- Containerization

Citrix Definition of containerization

Finally, you have the general definition given by everyone in the industry which is a bit more general and the underlying technology that would allow the usage listed in the paragraph above.

Containerization is defined as a form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS). A container is essentially a fully packaged and portable computing environment:

- Everything an application needs to run – its binaries, libraries, configuration files and dependencies – is encapsulated and isolated in its container.
- The container itself is abstracted away from the host OS, with only limited access to underlying resources – much like a lightweight virtual machine (VM).
- As a result, the containerized application can be run on various types of infrastructure—on bare metal, within VMs, and in the cloud—without needing to refactor it for each environment.

That is because there is less overhead during startup and no need to set up a separate guest OS for each application since they all share the same OS kernel. Because of this high efficiency, containerization is commonly used for packaging up the many individual microservices that make up modern apps.

IBM Defines it as:

Containerization has become a major trend in software development as an alternative or companion to virtualization. It involves encapsulating or packaging up software code and all its dependencies so that it can run uniformly and consistently on any infrastructure. The technology is quickly maturing, resulting in measurable benefits for developers and operations teams as well as overall software infrastructure.

Containerization allows developers to create and deploy applications faster and more securely. With traditional methods, code is developed in a specific computing environment which, when transferred to a new location, often results in bugs and errors. For example, when a developer transfers code from a desktop computer to a virtual machine (VM) or from a Linux to a Windows operating system. Containerization eliminates this problem by bundling the application code together with the related configuration files, libraries, and dependencies required for it to run. This single package of software or “container” is abstracted away from the host operating system, and hence, it stands alone and becomes portable—able to run across any platform or cloud, free of issues.

Sources:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 282, 290, 291, 444). Wiley. Kindle Edition.
- Citrix What is containerization and how does it work at:

  https://www.citrix.com/solutions/app-delivery-and-security/what-is-containerization.html

- IBM article on What is containerization at: https://www.ibm.com/cloud/learn/containerization

CONTINUOUS INTEGRATION AND CONTINUOUS DELIVERY (CI/CD)

First, just a few words about DEVOPS:

DevOps has a focus on agility, automation, rapid development, and frequent delivery of working software, based on this, new working styles emerged. These forces **coalesce** development with automation and aspects of system administration and operations. This integration of disciplines and technology has come to be known as DevOps.

DevOps breaks down the wall between developers and operations. **DevOps enables continuous integration and continuous deployment.**

DevOps accelerates software delivery and increases software quality and security. Many of the DevOps practices, such as process automation, emphasis on testing, and frequent deployments, are like those used in agile and iterative methodologies. The distinction between the two is that DevOps is an implementation of these practices and that this implementation can be used within the practice framework of the various methodologies.

Note from Clement: Coalesce means to unite into a whole

WHICH LEADS US TO CI AND CD

Continuous integration (CI) and continuous delivery (CD) embody a culture, set of operating principles, and collection of practices that **enable application development teams to deliver code changes more frequently and reliably**. The implementation is also known as the ***CI/CD* pipeline**.

CI/CD is one of the best practices for **devops teams** to implement. It is also an agile methodology best practice, as it enables software development teams to focus on meeting business requirements, code quality, and security because deployment steps are automated.

CI/CD defined

Continuous integration is a coding philosophy and set of practices that drive development teams to implement small changes and check in code to version control repositories frequently. Because most modern applications require developing code in different platforms and tools, the team needs a mechanism to integrate and validate its changes.

The technical goal of CI is to establish a consistent and automated way to build, package, and test applications. With consistency in the integration process in place, teams are more likely to commit code changes more frequently, which leads to better collaboration and software quality.

Continuous delivery picks up where continuous integration ends. CD automates the delivery of applications to selected infrastructure environments. Most teams work with multiple environments other than the production, such as development and testing environments, and CD ensures there is an automated way to push code changes to them.

CI/CD tools help store the environment-specific parameters that must be packaged with each delivery. CI/CD automation then performs any necessary service calls to web servers, databases, and other services that may need to be restarted or follow other procedures when applications are deployed.

Continuous integration and continuous delivery require *continuous testing* because the objective is to deliver quality applications and code to users. Continuous testing is often implemented as a set of automated regression, performance, and other tests that are executed in the CI/CD pipeline.

Source:

- For more into on CI/CD, see a nice article on the Infoworld.com website at:

  https://www.infoworld.com/article/3271126/what-is-cicd-continuous-integration-and-continuous-delivery-explained.html

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (pp. 774-775). Wiley. Kindle Edition.

CONTROL LOGICAL ACCESS TO APPLICATIONS

Note from Clement: This topic is **not** new within the CBK. It is related to Domain 5 on Identity and Access Management (IAM). Within domain five, they examine the core aspects of IAM, beginning with the foundational concept of controlling **physical and logical** access to assets. Including the essential practice of managing the identification and authentication of people, devices, and services. This topic would also include integrating identity as a third-party service and implementing and managing authorization mechanisms. Finally, it will include the identity and access provisioning lifecycle. As mentioned above, you must have both Physical and Logical access controls, or else you cannot claim to have security in place.

Logical access control tools are used for credentials, validation, authorization, and accountability in an infrastructure and the systems within. These components enforce access control measures for systems, applications, processes, and information. This type of access control can also be embedded inside an application, operating system, database, or infrastructure administrative system.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 483). Wiley. Kindle Edition.
- Logical Access Control, https://www.sciencedirect.com/topics/computer-science/logical-access-control

CRYPTO ATTACKS

NOTE FROM CLEMENT: Crypto Attacks have been in the CBK for many years. However, in this update they specifically listed 13 different attacks that you must be familiar with. Most of the books published will only cover a few and they do not cover the whole list. For your benefit I have them listed below with a short description.

In cryptography, the goal of the attacker is to break the secrecy of the encryption and learn the secret message and, even better, the secret key. There are dozens of different types of attacks that have been developed against different types of cryptosystems with varying levels of effectiveness. Some are easily understandable while others may require an advanced degree in mathematics to comprehend. Within the CBK, they cover some of the more common attacks.

Brute force

The simplest attack on a cipher is the brute force attack. In this attack, an attacker simply tries to decrypt the message with each possible secret key and checks the result of the decryption to see if it makes sense. Given enough time and computational resources, this attack is guaranteed to work since the true secret key must be within the set of possible secret keys and the attacker will eventually try it and (hopefully) realize that the resulting plaintext is the correct one.

Modern ciphers protect themselves against brute force attacks by using a secret key that is long enough to make guessing all the possibilities impossible. For example, the longest available key length of the AES cipher is 256 bits, which means there are 2^{256} possible AES keys. By contrast, there are an estimated 2^{266} atoms in the observable universe. No existing computer can search that size of a keyspace in a reasonable amount of time.

Ciphertext Only Attack (COA)

In this method, the attacker has access to a set of ciphertext(s). He does not have access to corresponding plaintext. COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext. Occasionally, the encryption key can be determined from this attack. Modern cryptosystems are guarded against ciphertext-only attacks.

Known Plaintext Attack (KPA)

In this method, the attacker knows the plaintext for some parts of the ciphertext. The task is to decrypt the rest of the ciphertext using this information. This may be done by determining the key or via some other method. The best example of this attack is *linear cryptanalysis* against block ciphers.

Frequency analysis Attack

In cryptanalysis, **frequency analysis** (also known as **counting letters**) is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.

Frequency analysis is based on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. Moreover, there is a characteristic distribution of letters that is roughly the same for almost all samples of that language.

For instance, given a section of English language, E, T, A and O are the most common, while Z, Q, X and J are rare. Likewise, TH, ER, ON, and AN are the most common pairs of letters (termed *bigrams* or *digraphs*), and SS, EE, TT, and FF are the most common repeats.
The nonsense phrase "ETAOIN SHRDLU" represents the 12 most frequent letters in typical English language text. In some ciphers, such properties of the natural language plaintext are preserved in the ciphertext, and these patterns have the potential to be exploited.

Chosen Ciphertext Attack (CCA)

A chosen-ciphertext attack is one in which cryptanalyst may choose a piece of ciphertext and attempt to obtain the corresponding decrypted plaintext. This type of attack is generally most applicable to **public-key cryptosystems.**

A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts. From these pieces of information, the adversary can attempt to recover the hidden secret key used for decryption.

Implementation attacks

An *implementation* attack exploits implementation weaknesses, such as in software, the protocol, or the encryption algorithm. Implementation attacks pose a serious threat to the security of cryptographic algorithms and protocols. In such attacks, not the abstract descriptions of cryptographic methods are attacked but their practical realizations in cryptographic devices. This opens a wide range of powerful attacks

Side-channel Attacks

A side channel attack breaks cryptography by using information leaked by cryptography, such as monitoring the electromagnetic field (EMF) radiation emitted by a computer screen to view information before it is encrypted in a van Eck phreaking attack, aka Transient Electromagnetic Pulse Emanation STandard (TEMPEST). Other well-known side channel attacks include spying on the power consumption of an electronic device to steal an encryption key, or acoustic attacks that record the sound of a user's keystrokes to steal their passphrase. Listening to a computer noise could also be used as a side channel attack.

Computers need power to run. The amount of power used and how long the power is used for can vary based upon the operations performed. When a cryptographic algorithm is being run on a computer, this may reveal information about the data being processed by the algorithm.

An example of a power analysis attack on a cryptographic algorithm is the Simple Power Analysis (SPA) of the RSA algorithm. In the RSA algorithm, the secret key is used as the power in an exponentiation operation. A simple way of performing this step is using the square-and-multiply algorithm. In square-and-multiply, the exponent (secret key) is represented in binary and walked through from most significant bit to least significant bit. If a bit is a zero, the current value is squared. If a bit is a one, the current value is squared and then multiplied by the base.

The difference between the operations performed for a zero bit and a one bit in the secret key makes a side-channel attack on this version of RSA possible.

Fault injection Attacks

Logical **attacks** are the number one threat for any secure embedded system. This means, **Fault Injection** is a **physical attack** on the logic with the goal to bypass secure boot mechanisms, extract a secret key, disrupt a program counter, and extract firmware or to manipulate any other secure asset inside an IC.

The easiest example of a Fault Injection as an attack is a voltage drop. If a device, or a specific chip normally needs 3.3 volts from a power supply, what could happen if during a sensitive operation (e.g., checking your PIN) we drop it to 2.2v more, or less? A few things can happen, either the devices continue working, or it mutes and needs to be reset, or even worse it breaks. But with the right timing it skips the verification and gives access to something normally not allowed, for example your bitcoin wallet data. This is what we would describe as a successful glitch. In general, we say: Every unprotected IC is vulnerable to Fault Injection Attacks.

Timing Attack

A timing attack on a cryptographic algorithm exploits the fact that the algorithm may take different amounts of time to run with different plaintexts or secret keys.

An example of a timing attack is the checking of a password during login to a secure system. Unprotected systems will incrementally check each character of the password for a match against the stored password and return failure immediately upon discovering mismatched characters. An attacker can try passwords starting with each of the possibilities for the first character of the password and select the option with the longest execution time (since it is the only case where the second character was also checked). By repeating this process one character at a time, the complete password can be built by the attacker.

Man-in-the-Middle (MITM)

The Man-in-the-Middle (MitM) attack assumes that an attacker, let us say Eve, can insert herself in the communication channel between Alice and Bob, who are trying to talk to one another. When Alice sends a message to Bob, Eve intercepts it before it reaches Bob. In a successful MitM attack, Eve can decrypt the intercepted message, read and possibly modify it, and then pass it on to Bob.

To pull off a Man-in-the-Middle attack, Eve typically needs to be able to convince Alice that Eve is Bob and Bob that Eve is Alice. Eve will then independently establish a separate secret key with each party and, when a message is moving from Alice to Bob, decrypts using her key for Alice and reencrypt using her key for Bob. As long as Eve controls the only communication channel between Alice and Bob, the MitM attack is undetectable.

Pass the hash

Pass the hash is a technique used to steal credentials and enable lateral movement within a target network. In Windows networks, the challenge-response model used by NTLM security is abused to enable a malicious user to authenticate as a valid domain user without knowing their password.

Even though Kerberos has replaced NTLM as the preferred authentication method for Windows domains, NTLM is still enabled in many Windows domains for compatibility reasons. And so, pass the hash attacks remain an effective tool in the hands of skilled attackers.

Kerberos exploitation and attacks

As far back as 2015, it was identified as one of the most dangerous attack techniques. Kerberos attacks are troublesome for three primary reasons:

Access: Once an attacker has Local Admin privileges, it is possible to dump additional credentials, which if left behind in the compromised machines, enable the attacker to move laterally in the network, elevate privileges and gain unauthorized access to valuable assets.

Obscurity: To bypass security controls and evade detection, an attacker can reuse Kerberos tickets to impersonate authorized users and sidestep authentication processes – disguising activity and avoiding authentication log traces.

Persistence: The days of stolen data being dumped all at once are largely over – attackers often prefer to remain on the network undiscovered for extended periods of time, funneling information out little –by – little. Kerberos attacks give attackers what they need most to do this: time. It is possible to maintain persistence with Kerberos tickets, even when credentials have been changed.

While there are several types of attacks on authentication protocols – including Pass-the-Hash, Overpass-the-Hash and Pass-the-Ticket – the most destructive of all is the Golden Ticket. Covering those attacks in great details is beyond the scope of this guide and not needed for the exam. After your exam, you can do deeper research if this is a topic of interest to you.

Ransomware (see RANSOMWARE further down in the document)

Other attacks not listed in the CBK:

Replay Attack

A replay attack is when an attacker replays a valid session between a legitimate user and some form of server. In this attack, Eve captures every piece of traffic between the user, Alice, and the server, Bob, during normal operation. Later, the attacker resends the first piece of traffic and waits for Bob's response before sending the next piece, and so on. If Bob does not implement some protection against replay attacks, Eve may be able to achieve a valid session with Bob while masquerading as Alice.

For example, assume that Alice is buying something from Bob's online store. The entire transaction process is encrypted, but Eve can make a copy of each stage of the communication between Alice and Bob. At the end of Alice's transaction, she has successfully purchased one bicycle. Now, Eve can begin to replay Alice's session with Bob. From Bob's perspective, Eve is actually Alice purchasing another bicycle from his store. Eve does not need to decrypt any of the traffic to perform a replay attack or even know what is going on, but she does have the ability to cause issues for Alice by draining her bank account or credit card and causing many bicycles to arrive at her residence.

To protect against replay attacks, many people who use ciphers in daily life (like Bob's store) will generate a random number to be included in each session. This way, if Bob sends the number to Alice and Alice sends it back, Bob can check that it is the expected number for the given session. When Eve attempts to replay Alice's session, she will provide the random number from Alice's session rather than the number for her replayed session and Bob will reject the transaction.
Encryption, Sequence Number, and Timestamps are tools that can prevent and minimize the danger of Replay Attacks.

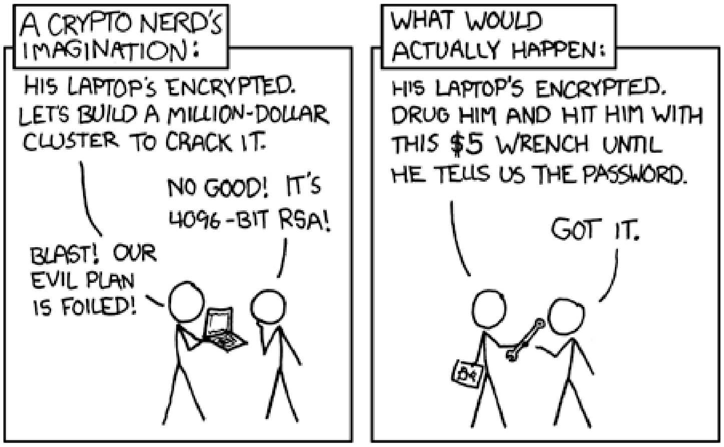
Chosen Plaintext Attack (CPA)

In this method, the attacker has the text of his choice encrypted. So, he has the ciphertext-plaintext pair of his choice. This simplifies his task of determining the encryption key. An example of this attack is *differential cryptanalysis* applied against block ciphers as well as hash functions.

Dictionary Attack

This attack has many variants, all of which involve compiling a 'dictionary'. In simplest method of this attack, attacker builds a dictionary of ciphertexts and corresponding plaintexts that he has learnt over a period of time. In the future, when an attacker gets the ciphertext, he refers the dictionary to find the corresponding plaintext. This is only effective against simple ciphers such as Code Book Mode ciphers.

Finally, Consider the human factor behind the technology:


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Graphic above from https://xkcd.com/538/

Source:

- https://www.commonlounge.com/discussion/4c8ace459d1840408e487a673cca255d
- https://www.tutorialspoint.com/cryptography/attacks_on_cryptosystems.htm
- https://en.wikipedia.org/wiki/Frequency_analysis
- https://www.linkedin.com/pulse/20141201173411-1571978-chosen-ciphertext-attack-cca/
- https://www.cyberark.com/resources/blog/kerberos-attacks-what-you-need-to-know
- https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

DATA LOSS PREVENTION (DLP)

Data loss prevention focuses on the detection and prevention of sensitive data exfiltration and/or lost data and includes use cases from a lost or stolen thumb drive to ransomware attacks. In a data loss, the data is gone and may or may not be recoverable.

Simply put, data loss is any loss of data whether intentional or accidental. If **you no longer have access to your data,** it has been lost.

Almost half of all data loss occurs as the result of hardware failure. These type failures can be a result of memory loss, power outages and even Mother Nature. Failure to secure data on offsite servers can prove to be disastrous if there is a power outage, flooding, fire or other unforeseen disaster.

Other losses occur when data is purposely or accidentally deleted. There are also the pesky malware viruses and worst of all computer hackers.

Like with data leakage, losses also can occur with employees taking work home. In this case, data is lost when an employee loses control of a laptop and there is no backup version of the data it contained.

DATA LEAKAGE PROTECTION (DLP)

Data leakage is more complex and includes the risk of sensitive data flowing between an organizations' critical systems, which are usually systems of records. While safeguards can be assumed to be in place in the "system of record", data leakage can occur when data is cascaded to complimentary systems unless the same level of data protection is enforced.

Some examples for systems of records are Human Resources (e.g., PeopleSoft, Workday, etc.), ERP (e.g. SAP, Oracle E-Business Suite, etc.), and CRM (e.g. SAP, Salesforce, etc.) systems. These critical applications may reside within your corporate network or exists as SaaS applications in the cloud.

Data leakage, also known as information leakage takes place when there is an unauthorized transmission of data from an organization. This data is then transmitted to someone outside of the company.

Data leakage is not always **intentional**. A data leak can begin when an employee takes a report home and accidentally leaves it on the train or bus. The leak occurs when someone comes along and takes the file.

An intentional leak is when data is purposely transmitted to someone **outside** the company who does not have a legal right to possess the information.

Leaks of information can be physical transfers or an electronic transmittal. A leak can also be as simplistic as someone memorizing data and using it outside the scope of their authority.

Source:

- Data loss can occur on any device that stores data.

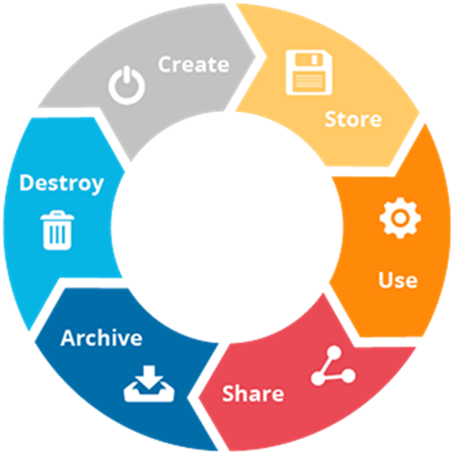
DATA LOCATION - DATA MAINTENANCE - DATA RETENTION

This is not new content; it is part of the data / information lifecycle. They added more details to it, and it is not a completely new topic. In fact, the exact names used can vary a bit from one source to another being studied. The important is to understand each of the steps at an extremely high level.

The policies and procedures of an organization provide rules for the handling of each category of information at the appropriate level of sensitivity throughout the lifetime of the asset. Handling rules for information should cover the access, transfer, and storage of sensitive data. It is important to maintain a consistent process for handling throughout the entire data lifecycle.

The security professional must be able to design and implement a records management program to provide ways to identify, maintain, and dispose of company records in a safe, timely, and cost-effective manner. The use of hierarchical storage management (HSM) is effective as a record storage technique to support a secure lifecycle management process.

- Data collection (Create)
- Data location (Store)
- Data maintenance (Use and Share)
- Data retention (Archive)
- Data remanence (Destroy)
- Data destruction (Destroy)



Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 209). Wiley. Kindle Edition.

DIGITAL RIGHTS MANAGEMENT (DRM)

This is not a new topic; it was simply added to the list of topics within the new CBK document.
The Official (ISC)² CISSP CBK Reference Guide has more than 25 mention of the term DRM.

Digital Rights Management (DRM) is the name applied to technology that permits the owner of intellectual property (documents, music, movies, etc.) to impose technical limits on how copies of that information may be used. There is considerable controversy over how and under what circumstances DRM technology is used, relative to the intellectual property rights of both the content creators and content consumers. Understanding the technical aspects of this technology will help security professionals legally and appropriately implement DRM in their environments.

Digital rights management (DRM) is a way to protect copyrights for digital media. This approach includes the use of technologies that limit the copying and use of copyrighted works and proprietary software.

In a way, digital rights management allows publishers or authors to control what paying users can do with their works. For companies, implementing digital rights management systems or processes can help to prevent users from accessing or using certain assets, allowing the organization to avoid legal issues that arise from unauthorized use. Today, DRM is playing a growing role in data security.

With the rise of peer-to-peer file exchange services such as torrent sites, online piracy has been the bane of copyrighted material. DRM technologies do not catch those who engage in piracy. Instead, they make it impossible (harder) to steal or share the content in the first place.

How does Digital Rights Management Works?

Most of the time, digital rights management includes codes that prohibit copying, or codes that limit the time or number of devices on which a certain product can be accessed.

Publishers, authors, and other content creators use an application that encrypts media, data, e-book, content, software, or any other copyrighted material. Only those with the decryption keys can access the material. They can also use tools to limit or restrict what users are able to do with their materials.

There are many ways to protect your content, software, or product.

DRM allows you to:

- Restrict or prevent users from editing or saving your content.
- Restrict or prevent users from sharing or forwarding your product or content.
- Restrict or prevent users from printing your content. For some, the document or artwork may only be printed up to a limited number of times.
- Disallow users from creating screenshots or screen grabs of your content.
- Set an expiry date on your document or media, after which the user will no longer be able to access it. This could also be done by limiting the number of uses that a user has. For instance, a document may be revoked after the user has listened ten times or opened and printed the PDF 20 times.
- Lock access only to certain IP addresses, locations, or devices. This means that if your media is only available to US residents, then it will not be accessible to people in other countries.
- Watermark artworks and documents in order to establish ownership and identity.
- Digital rights management also allows publishers and authors to access a log of people and times when certain media, content, or software was used. For instance, you can see when a particular e-book was downloaded or printed and who accessed it.

Challenges of Digital Rights Management

Not everybody agrees with digital rights management. For instance, users who pay for music on iTunes would love to be able to listen to the song on any device or use it in whatever way they wish.

On the other hand, businesses that pay thousands of dollars for a high-value industry report are willing to use DRM so that their competitors are unable to get the same report for free. Some critics of DRM have pointed out that this creates an unfair advantage for businesses that have money to burn because smaller operations may not be able to afford the information that they need to grow their businesses.

However, DRM technology is not a perfect solution. Even if copywrite holders incorporate digital rights management code into their product, the public may discover a way to work around it. For instance, if they make their content playable only on one player, some users will inevitably try to figure out the decryption keys and then create another player that can play the copyrighted content. Users then download the new player in the hopes of circumventing the DRM encryption. There are also free tools to remove DRM codes, which – while unethical – are readily available online.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 339). Wiley. Kindle Edition.
- https://digitalguardian.com/blog/what-digital-rights-management

APPLICATION SECURITY TESTING

Dynamic Application Security Testing (DAST)
Static Application Security Testing (SAST)

This is another topic that had more details added. It has been within the CBK for the past few versions, but terms such as DAST and SAST were not specifically listed. Application Security Testing is certainly one of the key issues we must deal with if you do any software development or even when you acquire software from third-party as well. It does not matter if it is open source or commercial software, any software could have vulnerabilities that may or may not be known to the final user.

Awareness and management of existing vulnerabilities as well as continuous education on security vulnerabilities impacting information is a must. Vulnerabilities exist for several reasons:

- The software code could be based on bad design.
- The quality of code could be poor.
- Secure and defensive coding may not have been a priority.
- The developers may not have either the knowledge or the interest to write secure code.
- It could also be that secure software processes and practices into its SDLC did not exist.

Each of these factors and others can cause vulnerabilities within the software to be created, packaged, and distributed.

Automated code scanning techniques are effective for discovering vulnerabilities across volumes of a code base. Common types of automated code coverage are Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST).

The differences between SAST and DAST include where they run in the development cycle and what kinds of vulnerabilities they find. You usually need both for full coverage.

Recent high-profile data breaches have made organizations more concerned about the financial and business consequences of having their data stolen. They know they need to identify vulnerabilities in their applications and mitigate the risks. So, they’re adding application security testing, including SAST and DAST, to their software development workflows.

What are SAST and DAST?

SAST and DAST are application security testing methodologies used to find security vulnerabilities that can make an application susceptible to attack.

Static Application Security Testing (SAST) is a white box method of testing. It examines the code to find software flaws and weaknesses such as SQL injection and others listed in the OWASP Top 10.

Dynamic Application Security Testing (DAST) is a black box testing method that examines an application as it is running to find vulnerabilities that an attacker could exploit.

Many organizations wonder about the Pros and Cons of choosing SAST vs. DAST.

SAST and DAST are different testing approaches with different benefits. They find different types of vulnerabilities, and they're most effective in different phases of the Software Development Life Cycle (SDLC).

SAST should be performed early and often against all files containing source code.

DAST should be performed on a running application in an environment similar to production.

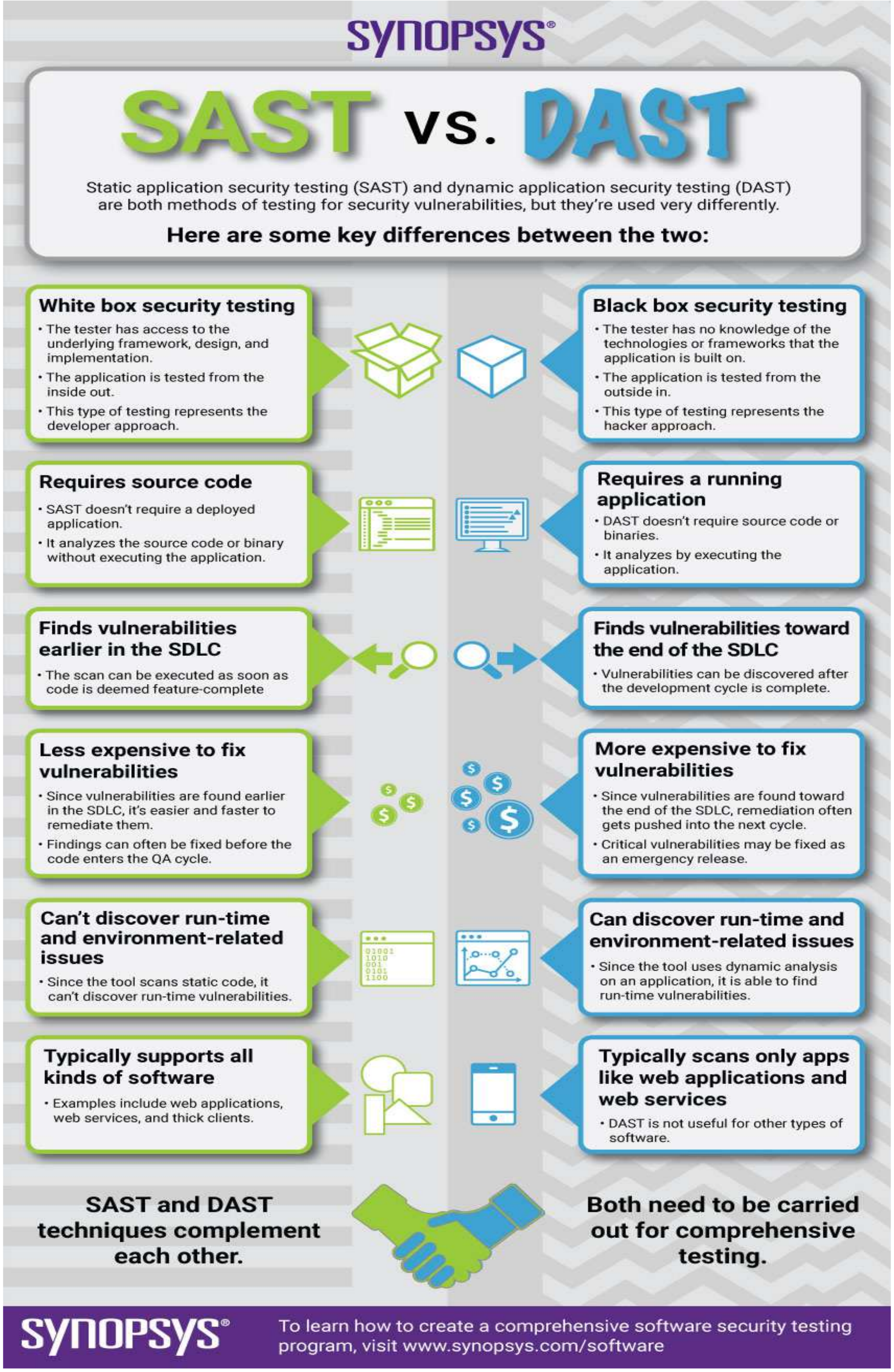
The best approach is to include both SAST and DAST in your application security testing program.

On the next page you have a nice graphic from Synopsis showing the difference between the two methodologies.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 839). Wiley. Kindle Edition.
- https://www.synopsys.com/blogs/software-security/sast-vs-dast-difference/

Comparison of SAST versus DAST by SYNOPSYS



SYNOPSYS®

SAST vs. DAST

Static application security testing (SAST) and dynamic application security testing (DAST) are both methods of testing for security vulnerabilities, but they're used very differently.

Here are some key differences between the two:

White box security testing

- The tester has access to the underlying framework, design, and implementation.
- The application is tested from the inside out.
- This type of testing represents the developer approach.

Black box security testing

- The tester has no knowledge of the technologies or frameworks that the application is built on.
- The application is tested from the outside in.
- This type of testing represents the hacker approach.

Requires source code

- SAST doesn't require a deployed application.
- It analyzes the source code or binary without executing the application.

Requires a running application

- DAST doesn't require source code or binaries.
- It analyzes by executing the application.

Finds vulnerabilities earlier in the SDLC

- The scan can be executed as soon as code is deemed feature-complete

Finds vulnerabilities toward the end of the SDLC

- Vulnerabilities can be discovered after the development cycle is complete.

Less expensive to fix vulnerabilities

- Since vulnerabilities are found earlier in the SDLC, it's easier and faster to remediate them.
- Findings can often be fixed before the code enters the QA cycle.

More expensive to fix vulnerabilities

- Since vulnerabilities are found toward the end of the SDLC, remediation often gets pushed into the next cycle.
- Critical vulnerabilities may be fixed as an emergency release.

Can't discover run-time and environment-related issues

- Since the tool scans static code, it can't discover run-time vulnerabilities.

Can discover run-time and environment-related issues

- Since the tool uses dynamic analysis on an application, it is able to find run-time vulnerabilities.

Typically supports all kinds of software

- Examples include web applications, web services, and thick clients.

Typically scans only apps like web applications and web services

- DAST is not useful for other types of software.

SAST and DAST techniques complement each other.

Both need to be carried out for comprehensive testing.

SYNOPSYS® To learn how to create a comprehensive software security testing program, visit www.synopsys.com/software

EDGE COMPUTING SYSTEMS

This is an interesting topic that was added to the latest CBK. We all heard at some point some buzz about Edge Computing, however many people do not really know what it is.

Edge computing is transforming the way data is being handled, processed, and delivered from millions of devices around the world. The explosive growth of internet-connected devices – the IoT – along with new applications that require real-time computing power, continues to drive edge-computing systems.

Faster networking technologies, such as 5G wireless, are allowing for edge computing systems to accelerate the creation or support of real-time applications, such as video processing and analytics, self-driving cars, artificial intelligence and robotics, to name a few.

While early goals of edge computing were to address the costs of bandwidth for data traveling long distances because of the growth of IoT-generated data, the rise of real-time applications that need processing at the edge will drive the technology ahead.

What is edge computing?

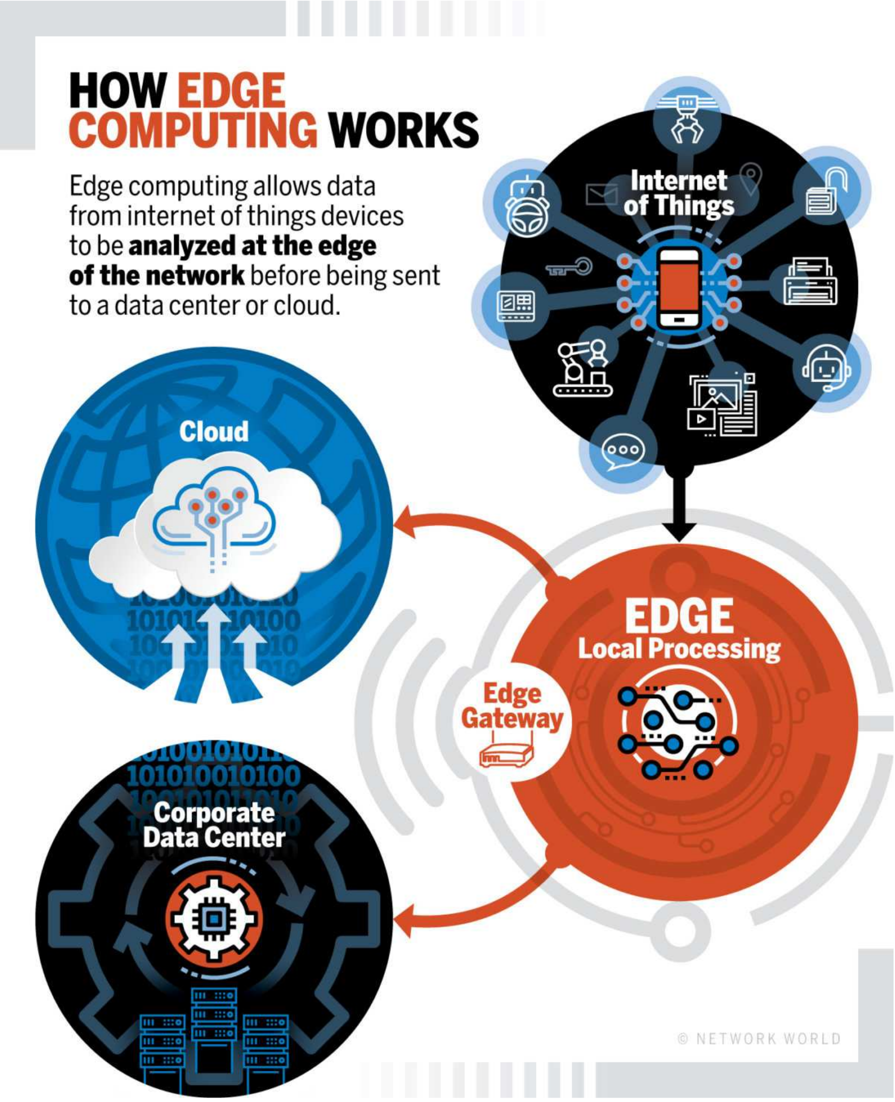
Gartner defines edge computing as “a part of a distributed computing topology in which information processing is located close to the edge – where things and people produce or consume that information.”

At its basic level, edge computing brings computation and data storage closer to the devices where it is being gathered, rather than relying on a central location that can be thousands of miles away. This is done so that data, especially real-time data, does not suffer latency issues that can affect an application’s performance. In addition, companies can save money by having the processing done locally, reducing the amount of data that needs to be processed in a centralized or cloud-based location.

Edge computing was developed due to the exponential growth of IoT devices, which connect to the internet for either receiving information from the cloud or delivering data back to the cloud. And many IoT devices generate enormous amounts of data during their operations.

Think about devices that monitor manufacturing equipment on a factory floor, or an internet-connected video camera that sends live footage from a remote office. While a single device producing data can transmit it across a network quite easily, problems arise when the number of devices transmitting data at the same time grows. Instead of one video camera transmitting live footage, multiply that by hundreds or thousands of devices. Not only will quality suffer due to latency, but the costs in bandwidth can be tremendous.

Edge-computing hardware and services help solve this problem by being a local source of processing and storage for many of these systems. An edge gateway, for example, can process data from an edge device, and then send only the relevant data back through the cloud, reducing bandwidth needs. Or it can send data back to the edge device in the case of real-time application needs.


HOW EDGE COMPUTING WORKS
Edge computing allows data from internet of things devices to be analyzed at the edge of the network before being sent to a data center or cloud.
Internet of Things
Cloud
EDGE
Local Processing
Edge Gateway
Corporate Data Center
© NETWORK WORLD

These edge devices can include many different things, such as an IoT sensor, an employee’s notebook computer, their latest smartphone, the security camera or even the internet-connected microwave oven in the office break room. Edge gateways themselves are considered edge devices within an edge-computing infrastructure.

Take a few minutes and watch the following video for a better understanding of Edge Computing and its benefits:

https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html?jwsource=cl

Source:

- https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html

EMBEDDED SYSTEMS

This topic was already covered within the official study book from ISC2. It is not something totally new. The latest CBK added this topic to the list of topics.

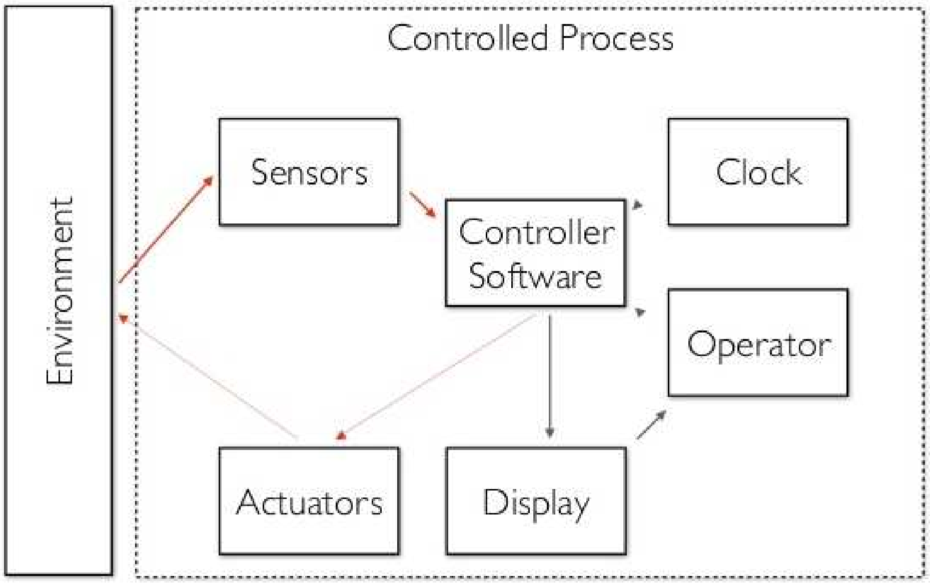
What is an Embedded System?

An embedded system is a microprocessor-based computer hardware system with software that is **designed to perform a dedicated function**, either as an independent system or as a part of a large system. At the core is an integrated circuit designed to carry out computation for real-time operations.
Complexities range from a single microcontroller to a suite of processors with connected peripherals and networks; from no user interface to complex graphical user interfaces. The complexity of an embedded system varies significantly depending on the task for which it is designed.

Embedded system applications range from digital watches and microwaves to hybrid vehicles and avionics. As much as 98 percent of all microprocessors manufactured are used in embedded systems.

Embedded systems can be found in a wide range of technologies. Embedded systems are dedicated information processing components embedded in larger mechanical or electrical systems, intended to provide a limited set of functions. The healthcare industry has innovated with embedded systems that provide great benefit to both care providers and patients.

One example is the tracking of patients and healthcare staff through a real-time location system (RTLS), fulfilled by active RFID tags and proximity sensors. Another example that truly embraces IoT-capable embedded devices is what is now known as “telehealth” or remote health monitoring. Most helpful for patients who cannot easily travel to a hospital, IoT-capable devices are brought to the patient’s home and communicate remotely with healthcare staff.



Assessing the vulnerabilities in an embedded system ought to start with an enumeration of the attack surfaces available, and then examining each. this examination can be done in several ways, including code inspection, threat modeling, and white- or black-box penetration testing.

Generally, these attack surfaces will fall into the following categories:

- User interface (buttons or other methods of user input)
- Physical attacks
- Sensor attacks
- Output attacks
- Processor attacks

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 292-293). Wiley. Kindle Edition.
- https://www.omnisci.com/technical-glossary/embedded-systems

ENCAPSULATION

NOTE FROM CLEMENT:
This topic is related to micro-segmentation. This is where you will find it in the CBK.

Encapsulation is an architectural concept where objects are accessed only through functions which logically separate functions that are abstracted from their underlying object by inclusion or information hiding within higher level objects. The functions might be specific to accessing or changing attributes about that object. The encapsulation functions can define the security policy for that object and mediate all operations on that object. Those functions act as sort of an agent for the object. Proper encapsulation requires that all access or manipulation of the encapsulated object must go through the encapsulation functions, and that it is not possible to tamper with the encapsulation of the object or the security attributes (e.g., permissions) of the encapsulation functions. Device drivers can be considered to use a form of encapsulation in which a simpler and consistent interface is if hides the details of a particular device, as well as the differences between similar devices.

Encapsulation refers to a programming approach that revolves around data and functions contained, or *encapsulated*, within a set of operating instructions. Applications become vulnerable to an attack when they fail to separate or differentiate critical data or functionality within components.

Another example of encapsulation is a capsule. Basically, capsule encapsulates several combinations of medicine. If combinations of medicine are **variables** and **methods,** then the capsule will act as a **class** and the whole process is called Encapsulation.

Encapsulation is not a **security** measure in that it prevents people from messing with your code. It is a **security** measure in the sense that people **can**'t go directly in and change variables without going through your proper channels.

Real Life Example

An example where encapsulation is used in the real world is the use of the setuid bit. Typically, in Linux or any Unix-like operating system, a file has ownership based on the person who created it. And an application runs based on the person who launched it. But a special mechanism, setuid, allows for a file or object to be set with different privileges. Setting the setuid bit on a file will cause it to open with the permission of whatever account you set it to be. The setuid bit controls access, above and beyond the typical operation. That is an example of encapsulation.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 224). Wiley. Kindle Edition.
- https://www.veracode.com/security/encapsulation-vulnerabilities
- https://www.scientecheasy.com/2020/07/encapsulation-in-java.html/
- https://stackoverflow.com/questions/56332669/what-is-the-purpose-of-encapsulation-does-it-provide-a-security-layer

ETHICAL DISCLOSURE (under generate test output and generate report)

What is ethical disclosure?

Vulnerability disclosure is the practice of publishing information related to a security vulnerability found in software. The purpose for such a disclosure is to inform the customer of the potential risks, so that they can take actions to minimize the effects of the vulnerability.

The question of whether or not to disclose a newly found vulnerability is one of the most sensitive decisions a software provider can make. As a trusted provider, we want to inform customers of issues that could impact their operations.

However, releasing too much information about a vulnerability too quickly could potentially result in an intruder using it to gain an upper hand against customers.

Companies providing software to customers should have a policy in place and the values clearly stated in the policy document in order to balances these two extremes.

NOTE FROM CLEMENT:
Ethical disclosure is a huge debate that will not be solved within this short paragraph. If this is something that interest you, do further study after your exam and find out all the details and how complex it can be. Especially, when you report some of your competitor's vulnerabilities which makes your produce shine or look better than theirs.

Source:

- https://www.osisoft.com/terms-and-conditions/ethical-disclosure

EXCEPTION HANDLING (under generate test output and generate report)

This may seem like a new topic for some of you, but it is not. This is part of the Design Principles contained within ISO 19249 “Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications.” Published in 2017 by the International Organization for Standardization (ISO) published its first revision of the standard. It is covered in great details within the latest ISC2 study reference, see reference further below.

The aim of ISO 19249 is to describe architectural and design principles to be used to foster the secure development of systems and applications. ISO 19249 specifies five architectural principles and five design principles.

The five architectural principles from ISO/IEC 19249 are:

Domain separation

A domain is a concept that describes enclosing a group of components together as a common entity. As a common entity, these components, be they resources, data, or applications, can be assigned a common set of security attributes. The principle of domain separation involves:

Placing components that share similar security attributes, such as privileges and access rights, in a That domain can then be assigned the necessary controls deemed pertinent to its components.

Only permitting separate domains to communicate over well-defined and (completely) mediated communication channels (e.g., APIs).

In networking, the principle of domain separation can be implemented through net- work segmentation – putting devices which share similar access privileges on the same distinct network, connected to other network segments using a firewall or other device to mediate access between segments (domains).

Layering

Layering is the hierarchical structuring of a system into different levels of abstraction, with higher levels relying upon services and functions provided by lower levels, and lower levels hiding (or abstracting) details of the underlying implementation from higher levels.

Encapsulation

Encapsulation is an architectural concept where objects are accessed only through functions which logically separate functions that are abstracted from their underlying object by inclusion or information hiding within higher level objects. The functions might be specific to accessing or changing attributes about that object. The encapsulation functions can define the security policy for that object and mediate all operations on that object. Those functions act as sort of an agent for the object.

Proper encapsulation requires that all access or manipulation of the encapsulated object must go through the encapsulation functions, and that it is not possible to tamper with the encapsulation of the object or the security attributes (e.g., permissions) of the encapsulation functions.

Redundancy

Redundancy is designing a system with replicated components so that the system can continue to operate despite errors or excessive load. From a security perspective, redundancy is an architectural principle for addressing possible availability compromises. In the case of replicated data stores, the challenge is to ensure consistency.

Virtualization

Virtualization is a form of emulation in which the functionality of one real or simulated device is emulated on a different one. More commonly, virtualization is the provision of an environment that functions like a single dedicated computer environment but supports multiple such environments on the same physical hardware. The emulation can operate at the hardware level, in which case we speak of virtual machines, or the operating system level, in which case we speak of containers.

The five design principles from ISO/IEC 19249 are:

Least privilege

Perhaps the most well-known concept of ISO/IEC 19249's design principles, least privilege is the idea to keep the privileges of an application, user, or process to the minimal level that is necessary to perform the task.

The purpose of ISO/IEC this principle is to minimize damage, whether by accident or malicious act. Users should not feel any slight from having privileges reduced, since their liability is also reduced in the case where their own access is used without their authorization. Implementing the principle is not a reflection of distrust, but a safeguard against abuse.

Attack surface minimization

A system's attack surface is its services and interfaces that are accessible externally (to the system). Reducing the number of ways, the system can be accessed, it can include:

1. disabling or blocking unneeded services and ports, using IP whitelisting to limit access

to internal API calls that need not be publicly accessible, and so on.

2. System hardening, the disabling and/or removal of unneeded services and components, is a form of attack surface minimization. This can involve blocking networking ports, removing system daemons, and otherwise ensuring that the only services and programs that are available are the minimum set necessary for the system to function as required.

3. Reducing the number of unnecessary open ports and running applications is an obvious approach. But another, less frequently observed strategy for minimizing the attack surface is to reduce the complexity of necessary services. If a service or function of a system is required, perhaps the workflow or operation of that service can be “minimized” by simplifying it.

Centralized parameter validation

The discussion of common system vulnerabilities would include parameter validation or data input validation. Many threats involve systems accepting improper inputs. Since ensuring that parameters are valid is common across all components that process similar types of parameters, using a single library to validate those parameters enables the necessary capability to carefully review and test that library.

Full parameter validation is especially important when dealing with user input, or input from systems to which users input data. Invalid or malformed data can be fed to the system, either unwittingly, by inept users, or by malicious attackers.

Examples where centralized parameter validation is used in the real world include the following:

- Validating input data by secure coding practices
- Screening data through an application firewall

Centralized general security services

The principle of centralizing security services can be implemented at several levels. At the operating system level, your access control, user authentication and authorization, logging, and key management are all examples of discrete security services that can and should be managed centrally. Simplifying your security services interface instead of managing multiple interfaces is a sensible benefit.

Implementing the principle at an operational or data flow level, one example is having a server dedicated for key management and processing of cryptographic data. The insecure scenario is one system sharing both front-end and cryptographic processing; if the front-end component were compromised, that would greatly raise the vulnerability of the cryptographic material.

Preparing for error and exception handling

Errors happen. Systems must ensure that errors are detected, and appropriate action taken, whether that is to just log the error or to take some action to mitigate the impact of the issue. Errors ought not to leak information, for example, by displaying stack traces or internal information in error reports that might disclose confidential information or provide information useful to an attacker. Systems must be designed to fail safe (as discussed earlier) and to always remain in a secure state, even when errors occur.

Errors can also be indicators of compromise and detecting and reporting such errors can enable a quick response that limits the scope of the breach.

An example of where error and exception handling are used in the real world is developing applications to properly handle errors and respond with a corresponding action.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 221-228). Wiley. Kindle Edition.

- At the link below you have a nice overview of the principles and what they mean: https://info-savvy.com/cissp-iso-iec-19249-bk1d3t1st2/

FIBER CHANNEL OVER ETHERNET (FCoE)

FCoE (Fiber Channel over Ethernet) is a storage protocol that enables Fiber Channel (FC) communications to run directly over Ethernet. FCoE makes it possible to move Fiber Channel traffic across existing high-speed Ethernet infrastructure and converges storage and IP protocols onto a single cable transport and interface.

The goal of FCoE is to consolidate I/O (input/output) and reduce switch complexity, as well as to cut back on cable and interface card counts. Adoption of FCoE has been slow, however, due to a scarcity of end-to-end FCoE devices and a reluctance on the part of many organizations to change the way they implement and manage their networks.

Traditionally, organizations have used Ethernet for Transmission Control Protocol/Internet Protocol (TCP/IP) networks and FC for storage networks. Fiber Channel supports high-speed data connections between computing devices that interconnect servers with shared storage devices and between storage controllers and drives. FCoE shares Fiber Channel and Ethernet traffic on the same physical cable or lets organizations separate Fiber Channel and Ethernet traffic on the same hardware.

FCoE uses a lossless Ethernet fabric and its own frame format. It retains Fiber Channel's device communications but substitutes high-speed Ethernet links for Fiber Channel links between devices.

FCoE works with standard Ethernet cards, cables and switches to handle Fiber Channel traffic at the data link layer, using Ethernet frames to encapsulate, route and transport FC frames across an Ethernet network from one switch with Fiber Channel ports and attached devices to another, similarly equipped switch.

FCoE is often compared to iSCSI (Internet Small Computer System Interface), an IP-based storage networking standard.

How Fiber Channel over Ethernet works

As previously noted, FCoE works by sending Fiber Channel packets across an Ethernet network. It accomplishes this by encapsulating the native Fiber Channel packets inside of Ethernet packets.

To make this work, a special type of network adapter called a converged network adapter -- also known as CAN or C-NIC -- is used. A converged network adapter is a special type of network adapter that combines the functionality of a Fiber Channel host bus adapter with that of an Ethernet network adapter.

This converged adapter not only provides the required physical connectivity, but it also enables lossless Ethernet. This is essential because Fiber Channel is a lossless protocol, and storage area networks (SANs) expect lossless communications.

Source:

- See a nice video at: https://youtu.be/R94U0_iZK4A
- https://searchstorage.techtarget.com/definition/FCoE-Fibre-Channel-over-Ethernet

HIGH-PERFORMANCE COMPUTING (HPC) SYSTEMS

High-performance computing (HPC) is the ability to process data and perform complex calculations at high speeds. To put it into perspective, a laptop or desktop with a 3 GHz processor can perform around 3 billion calculations per second. While that is much faster than any human can achieve, it pales in comparison to HPC solutions that can perform quadrillions of calculations per second.

One of the best-known types of HPC solutions is the supercomputer. A supercomputer contains thousands of compute nodes that work together to complete one or more tasks. This is called parallel processing. It is similar to having thousands of PCs networked together, combining compute power to complete tasks faster.

Why is HPC important?

It is through data that groundbreaking scientific discoveries are made, game-changing innovations are fueled, and quality of life is improved for billions of people around the globe. HPC is the foundation for scientific, industrial, and societal advancements.

As technologies like the Internet of Things (IoT), artificial intelligence (AI), and 3-D imaging evolve, the size and amount of data that organizations have to work with is growing exponentially. For many purposes, such as streaming a live sporting event, tracking a developing storm, testing new products, or analyzing stock trends, the ability to process data in real time is crucial.

To keep a step ahead of the competition, organizations need lightning-fast, highly reliable IT infrastructure to process, store, and analyze massive amounts of data.

How does HPC work?

HPC solutions have three main components:

- Compute
- Network
- Storage

To build a high-performance computing architecture, compute servers are networked together into a cluster. Software programs and algorithms are run simultaneously on the servers in the cluster. The cluster is networked to the data storage to capture the output. Together, these components operate seamlessly to complete a diverse set of tasks.

To operate at maximum performance, each component must keep pace with the others. For example, the storage component must be able to feed and ingest data to and from the compute servers as quickly as it is processed. Likewise, the networking components must be able to support the high-speed transportation of data between compute servers and the data storage. If one component cannot keep up with the rest, the performance of the entire HPC infrastructure suffers.

What is an HPC cluster?

An HPC cluster consists of hundreds or thousands of compute servers that are networked together. Each server is called a node. The nodes in each cluster work in parallel with each other, boosting processing speed to deliver high-performance computing.

HPC use cases

Deployed on premises, at the edge, or in the cloud, HPC solutions are used for a variety of purposes across multiple industries. Examples include:

- Research labs . HPC is used to help scientists find sources of renewable energy, understand the evolution of our universe, predict and track storms, and create new materials.
- Media and entertainment . HPC is used to edit feature films, render mind-blowing special effects, and stream live events around the world.
- Oil and gas . HPC is used to more accurately identify where to drill for new wells and to help boost production from existing wells.
- Artificial intelligence and machine learning. HPC is used to detect credit card fraud, provide self-guided technical support, teach self-driving vehicles, and improve cancer screening techniques.
- Financial services. HPC is used to track real-time stock trends and automate trading.
- HPC is used to design new products, simulate test scenarios, and make sure that parts are kept in stock so that production lines are not held up.
- HPC is used to help develop cures for diseases like diabetes and cancer and to enable faster, more accurate patient diagnosis.

Source:

- https://www.acecloudhosting.com/blog/high-performance-computing/
- https://www.netapp.com/data-storage/high-performance-computing/what-is-hpc/

SECURITY IMPACT OF ACQUIRED SOFTWARE

When an organization acquires software, it also acquires the risks inherent in or related to that software. When an organization acquires software, it also acquires the product of the skills and habits of the developers. It receives the management effectiveness, or lack thereof, of the company or community that developed it. It might inherit malware in its envelope.

There are different types of software. Some software is **commercial off-the-shelf** software. Other software is **provided by a vendor**. **OSS** is another type. Even if an organization develops software internally, it often requires libraries and packages developed externally for necessary functionality. Even after an organization assesses the software products that it already uses, the products require updates and patches. These are all sources of acquired software. And if one organization acquires another one, the acquisition may come with all these forms of software. That is why it's important to assess acquired software.

Commercial-off-the-shelf (COTS) Software / Third Party Software

Commercial off-the-shelf (COTS) software is software that is ready made and available to the public for sale. It can be purchased outright with a license or leased. It may come with vendor support. An advantage of COTS is that it can immediately fulfill a business or technical need at a low cost. The downside of COTS is that it can come with vulnerabilities, and some can affect the organization's information systems once installed and used.

Open-Source Software (OSS)

There are many benefits to OSS. First, OSS is often free or more affordable than commercial software. Depending on the software, it can also offer flexibility to modify the program source code to meet your needs. Open source is typically supported by an active community of developers. And it is (arguably) secure. On the other hand, the downsides of OSS include its complexity, the fact that it often requires technical expertise and a thorough evaluation process, and that it is (potentially) insecure. (There are two sides to the security/insecurity argument, each with its own merits.)

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 835). Wiley. Kindle Edition.

INTEGRATED DEVELOPMENT ENVIRONMENT (IDE)

What is an IDE?

An IDE, or Integrated Development Environment, enables programmers to consolidate the different aspects of writing a computer program.

IDEs increase programmer productivity by combining common activities of writing software into a single application: editing source code, building executables, and debugging.

Editing Source Code

Writing code is an important part of programming. We start with a blank file, write a few lines of code, and a program is born! IDEs facilitate this process with features like syntax highlighting and autocomplete.

Syntax Highlighting

An IDE that knows the syntax of your language can provide visual cues.

Words that have special meaning like class in Java, are highlighted with different colors.

Compare these two code samples:

Syntax highlighting makes code easier to read by visually clarifying different elements of language syntax.

Autocomplete

When the IDE knows your programming language, it can anticipate what you are going to type. For example, It may autocomplete Statements such as System.out.println().

In an IDE, we might see System as an autocomplete option after only typing Sy. This saves keystrokes so the programmer can focus on logic in their code.

Building Executables

Java is a compiled language. Before programs run, the source code of a **.java** file must be transformed into an executable **.class** by the compiler. Once compiled, the program can be run from the terminal.

This compilation process is necessary for every program, so why not have the IDE do it for us? IDEs provide automated build processes for languages, so the act of compiling and executing code is abstracted away.

Debugging

No programmer can avoids writing bugs and programs with errors.

When a program does not run correctly, the IDE provide debugging tools that allow programmers to examine different variables and inspect their code in a deliberate way.

IDEs also provide hints while coding to prevent errors **before** compilation.

Coding on Your Computer

The biggest benefit to using an IDE is that it allows you to code and run Java programs on your own computer.

Use Cases

There are many different technical and business use cases for IDEs, which likewise means there are many proprietary and open-source IDE options on the market. Typically, the most important differentiating characteristics between IDEs are:

- **The number of supported languages**: Some IDEs are dedicated to one language, and so are a better match for a specific programming paradigm. IntelliJ, for instance, is known primarily as a Java IDE. Other IDEs have a broad array of supported languages all in one, like the Eclipse IDE which supports Java, XML, Python, and others.

- **Supported operating system(s)**: A developer's operating system will constrain which IDEs are viable (unless an IDE is cloud-based), and if the application being developed is intended for an end user with a specific operating system (like Android or iOS), this may be an additional constraint.
- **Automation features**: Even though most IDEs include the 3 key features of a text editor, build automation, and debugger, many include support for additional features like refactoring, code search, and continuous integration and continuous deployment (CI/CD) tools.
- **Impact on system performance**: An IDE's memory footprint may be important to consider if a developer wants to run other memory-intensive applications concurrently.

- **Plugins and extensions**: Some IDEs include the ability to customize workflows to match a developer's needs and preferences.

Mobile development IDEs

Nearly every industry has been affected by the rising popularity of apps designed for smartphones and tablets, leading many companies to develop mobile apps in addition to traditional web apps. One of the key factors in mobile application development is platform choice. For instance, if a new application is intended for use on iOS, Android, and a web page, it may be best to start with an IDE that provides cross-platform support for multiple operating systems.

Cloud IDEs

IDEs that are provided as a cloud-based Software-as-a-Service (SaaS) provide a number of unique benefits compared to local development environments. For one, as with any SaaS offering, there is no need to download software and configure local environments and dependencies, so developers can start contributing to projects quickly. This also provides a level of standardization across team members' environments, which can mitigate the common "this works on my machine, why doesn't it work on yours" problem. Additionally, since the development environment is centrally managed, no code resides on an individual developer's computer, which can help with intellectual property and security concerns.

The impact of processes on local machines is also different. Processes like running builds and testing suites are typically compute-intensive, which means developers are probably unable to continue using workstations while a process is running. A SaaS IDE can dispatch long-running jobs without monopolizing the compute resources of a local machine. Cloud IDEs are also typically platform agnostic, allowing connection to different cloud vendors.

Source:

- https://www.codecademy.com/articles/what-is-an-ide
- https://www.redhat.com/en/topics/middleware/what-is-ide

INTERNET SMALL COMPUTER SYSTEMS (iSCSI)

iSCSI stands for Internet Small Computer Systems Interface. iSCSI is a transport layer protocol that works on top of the Transport Control Protocol (TCP). It enables block-level SCSI data transport between the iSCSI initiator and the storage target over TCP/IP networks. iSCSI supports encrypting the network packets, and decrypts upon arrival at the target.

SCSI is a block-based set of commands that connects computing devices to networked storage, including spinning up storage media and data reads/writes.

The protocol uses initiators to send SCSI commands to storage device targets on remote servers. Storage targets may be SAN, NAS, tape, general-purpose servers – both SSD and HDD – LUNs, or others. The protocol allows admins to better utilize shared storage by allowing hosts to store data to remote networked storage, and virtualizes remote storage for applications that require direct attached storage.

iSCSI Target

iSCSI transports packets across TCP/IP networks. The iSCSI target is the remote storage, which appears to the host system as a local drive. The iSCSI protocol links the hosts and storage over IP networks: LAN, WAN, and Internet.

When the packets arrive at the iSCSI target, the protocol disassembles the packets to present SCSI commands to the operating system. If iSCSI has encrypted the network packet, it decrypts the packet at this stage.

iSCSI Performance

iSCSI performance is highly dependent on underlying technologies like 10 Gigabit Ethernet (10 GbE) and bridging technology in the data center.

10 GbE. Ethernet network connection speed has the single largest impact on iSCSI performance. Although smaller networks may run iSCSI protocols over 1 GbE networks, the slower speed is insufficient for mid-sized or enterprise data centers. Admins may increase some performance on a sub-10 GbE network by adding multiple NICs, but a single switch will not boost speed for multiple iSCSI ports. 10 GbE is the recommended speed for an enterprise storage environment. Because it is a wider pipe, there is little call for multiple NICs. Instead, adding server-class network adapters will accelerate iSCSI packets traveling the 10 GbE network.

Data center bridging. Bridging is a set of Ethernet extensions that protect SCSI traffic against data loss. This allows iSCSI to better compete with highly reliable Fiber Channel, which has run over lossless connections for years.

Multipathing. Multipathing I/O speeds up iSCSI network packets, and most operating systems support the technology. Typical iSCSI multipathing features assign multiple addresses to a single iSCSI session, which accelerates data transport.

Jumbo frames. These 9000-byte frames relieve congestion on slower Ethernet networks that are not using 10 GbE, which gives a performance boost of about 10-20 percent. Jumbo frames will not give much of a performance boost in 10 GbE, if any.

iSCSI and Fiber Channel: Two Main Approaches to Storage Data Transmission

iSCSI and Fiber Channel (FC) are leading methods of transmitting data to remote storage. In general, FC is a high-performance but expensive storage network that requires specialized admin skill sets. iSCSI is less expensive and simpler to deploy and manage but has higher latency.

There are additional protocols that merge the two. The best-known include Fiber Channel over IP (FCIP), a tunneling protocol for SAN-to-SAN replication that wraps the FC frame onto the TCP stream; and Fiber Channel over Ethernet (FCoE) that enables FC SANs to transport data packets over Ethernet networks.

Source:

- https://www.enterprisestorageforum.com/hardware/what-is-iscsi-and-how-does-it-work/

JUST-IN-TIME (JIT) ACCESS

This is a topic that falls under "Manage identification and authentication of people, devices, and services".

Using the just-in-time (JIT) access methodology, organizations can give elevate human and non-human users in real-time to provide elevated and granular elevated privileged access to an application or system in order to perform a necessary task. Cybersecurity industry analysts recommend JIT access as a way of provisioning secure privileged access by minimizing standing access.

JIT access helps organizations provision access so that users only have the privileges to access to privileged accounts and resources when they need that access and not otherwise any other times. Instead of granting always-on (or standing) access, organizations can use JIT access to limit access to a specific resource for a specific timeframe. This granular approach mitigates the risk of privileged account abuse by significantly reducing the amount of time a cyber attacker or malicious insider has to gain access to privileged accounts before moving laterally through a system and gaining unauthorized access to sensitive data.

JIT access can be seen as a way used to enforce the principle of least privilege to ensure users and non-human identities are given the minimum level of privileges. JIT access can also ensure that privileged activities are conducted in accordance with an organization's Identity Access Management (IAM), IT Service Management (ITSM) and Privileged Access Management (PAM) policies along with its entitlements and workflows. It is essential that any JIT access strategy enables organizations to maintain a full audit trail of privileged activities. This way organizations can easily identify who or what gained access to which systems, what they did at what time and for how long. Some agent-based privileged access management solutions provide organizations with the additional ability to actively monitor sessions and terminate risky privileged sessions in real time.

Types of Just-In-Time Access

Broker and remove access. This approach enables the creation of policies that require users to provide a justification for connecting to a specific target for a defined period of time. Typically, these users have a standing, privileged shared account and credentials for that account are managed, secured and rotated in a central vault.

Ephemeral accounts. These are one-time-use accounts, which are created on the fly and immediately deprovisioned or deleted after use.

Temporary elevation. This approach allows the temporary elevation of privileges, enabling users to access privileged accounts or run privileged commands on a by-request, timed basis. Access is removed when time is up.

How to Enable Just-In-Time Access

Following is a typical workflow for enabling JIT access. Keep in mind that users start out with zero standing access – i.e., no privileges by default:

A human or non-human user requests privileged access to a server, virtual machine or network device.

The request is verified against a pre-approval policy or is reviewed by an administrator who has the power to grant or deny the request for short-term privileged access. This approvals process can be automated to reduce friction for end-users and operations teams.

After gaining approval, the human or machine user is elevated to the access needed to enter the system and perform their specified task. This access can last for only a few minutes or for a few months, depending on the user's specific task(s) and the organization's governance policies.

After the task is complete, the user logs off and their access is revoked or deleted until it is needed again.

Why is Just-In-Time Access Important for Your Organization?

It helps organizations improve their overall cybersecurity posture by significantly reducing the risk of privileged access abuse and lateral movement by threat actors.

It helps simplify the administrator experience by removing the need for review cycles and wait days while still maintaining current workflows.

It helps improve compliance and simplifies auditing by minimizing the number of privileged users and privileged sessions and providing full audit trails of all privileged activities.

How to Implement Just-in-Time Access in Your Organization

To enforce just-in-time access, organizations typically take one or some of the following steps:

- Maintain a standing, privileged shared account with credentials that are centrally managed and regularly rotated.
- Create granular policies that require human and non-human users to provide specific justification for connecting to target systems and applications that house sensitive data, for specific periods of time.
- Record and audit privileged activity across all ephemeral accounts and enable alerting and response to anomalous behavior or activity.

- Enable the temporary elevation of privileges to allow human and non-human users to access specific privileged credentials and accounts or to run privileged commands.

The use of just-in-time access to enforce the principle of least privilege is an important part of Zero Trust. Zero Trust models demand that organizations verify anything and everything trying to connect to systems before granting access. As many organizations accelerate their digital transformation strategies, they are shifting from traditional perimeter security approaches to the Zero Trust framework to protect their most sensitive information and data.

Source:

- https://www.cyberark.com/what-is/just-in-time-access/

LESSONS LEARNED

(under Business Continuity, Disaster Recovery, as well as Incident Response)

Lesson learned are part of the maintenance of your plans. You avoid doing the same mistake twice and you can also learn from others mistakes as well before they may affect your business.

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to the BCP and DRP plans.

It is the responsibility of each BCP and DRP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the BCP or DRP Coordinator.

Types of documentation that should be generated and collected after a plan is activated include:

- Activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities;
- Functionality and data testing results;
- Lessons learned documentation; and
- After Action Report.

Event documentation procedures should detail responsibilities for development, collection, approval, and maintenance.

The incident management process has seven steps, and the last step is about Lessons Learned:

1. detection,
2. response,
3. mitigation,
4. reporting,
5. recovery,
6. remediation, and
7. lessons learned

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 651). Wiley. Kindle Edition.
- https%3A%2F%2Fnvlpubs.nist.gov%2Fnistpubs%2Flegacy%2Fsp%2Fnistspecialpublication800-34r1.pdf&usg=AOvVaw1fwYzlYDdlOh7JIF1iSK8l
- NIST 800-34 Rev 1 https://www.nist.gov/privacy-framework/nist-sp-800-34

LIBRAIRIES (In software Security Controls under software development)

Libraries in programming languages are collections of prewritten code that users can use to optimize tasks.

Library examples:

Here are a few programming library examples you might encounter in Python, JavaScript, and other languages.

NumPy

Primary Language: Python

Use: NumPy is a library used to make powerful arrays. For machine learning, NumPy divides the data and manipulates it easily.

Meaning, machine learning uses many operations on arrays of data. These data sets often contain thousands of numbers and to iterate through every single value one at a time would be difficult and lengthy. NumPy simplifies all of this!

Matplotlib

Primary Language: Python

Use: Going off of the above, Matplotlib is used with NumPy to help with datasets. Specifically, Matplotlib handles large datasets and comes complete with standard graphing functions. It’s also useful for visualizing values over time.

Basically, Matplotlib is great for plotting and works together with NumPy.

TensorFlow

Primary Language: Python or C++

Use: TensorFlow is a library developed by Google to facilitate the creation and training of machine learning models and neural networks. It can be used to create and train machine learning models.

Source:

- https://www.idtech.com/blog/what-are-libraries-in-coding

Li-Fi

LiFi, which stands for **Li**ght **Fi**delity, is a wireless communications technology that uses visible light to transmit data in real time. It is up to 100 times faster than standard Wi-Fi.

LiFi is a mobile wireless technology that uses light rather than radio frequencies to transmit data. The technology is supported by a global ecosystem of companies driving the adoption of LiFi, the next generation of wireless that is ready for seamless integration into the 5G core.

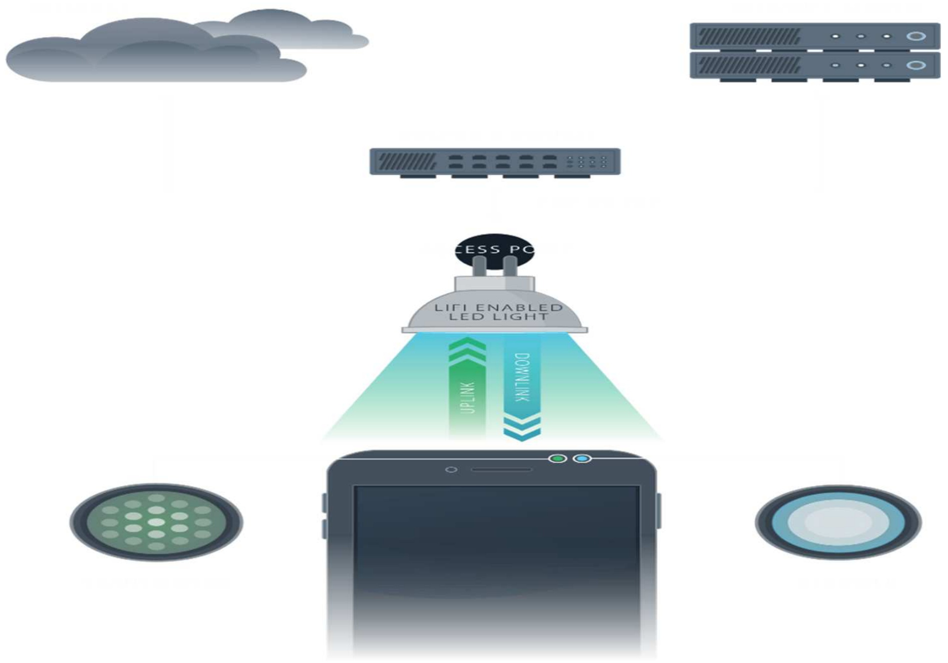
Radio frequency communication requires radio circuits, antennas and complex receivers, whereas LiFi is much simpler and uses direct modulation methods similar to those used in low-cost infrared communications devices such as remote-control units. LED light bulbs have high intensities and therefore can achieve large data rates.

Because it runs on light waves from common household LED bulbs, LiFi technology operates the way light does. Visible light has a much wider bandwidth than Wi-Fi, meaning that LiFi-enabled devices can send and receive huge volumes at extremely high speeds — up to 224 gigabits per second.

However, light cannot travel through walls because the light waves are too small. Additionally, to send and receive light signals, your light source must be active for the technology to work. So, if you're running your smart home on LiFi alone, you'd need to have LED bulbs throughout your house.

Yet by the same token, LiFi offers more security than Wi-Fi because of the opportunity to introduce physical barriers. You can contain light within a space, so you can protect the messages you're sending and receiving from outside parties.

LiFi signals are also immune to the electromagnetic interference that can plague radio frequency-sensitive areas. If you turn on your microwave or cordless phone near a LiFi signal, likewise, you will not disrupt an important transmission.



802.11 bb Global Light Communications Standards

The objective is to extend 802.11 to include the light medium. A standard with input across the Wi-Fi ecosystem 802.11bb TG aiming to deliver standard by mid-2021.

Source:

- https://purelifi.com/lifi-technology/
- https://www.verypossible.com/insights/what-is-lifi-and-how-does-it-work

LOG MANAGEMENT (Conduct logging and monitoring activities)

This is certainly NOT a new topic with the CBK. It was added within Domain 7 as 7.2 Conduct logging and monitoring activities. There are a lot of content in most security books about this topic. So, I will keep it short, and you can refer to your study book or the next standard mentioned below.

Proper logging will provide you with evidence of activities taking place over your networks, systems, services, and more.

Keeping reliable copies of our logs would also fall under your Data retention requirements. That also includes your Security and IT operations audit logs.

NIST SP 800-92, “Guide to Computer Security Log Management,” offers guidance on log archival, log retention, and log preservation.

Data retention requirements are based on factors such as operational need, legal requirements, and, in some cases, a specific incident or event that requires an exception to log management policy.

Assessments and audits need to look at more than just whether logs are captured and their content. In fact, assessments that consider log reviews look at items including the following:

- What logs are captured?
- How is log integrity ensured?
- Are log entries hashed and validated?
- Are the systems and applications that generate logs properly configured?
- Do logging systems use a centralized time synchronization service?
- How long are logs retained for, and does that retention time period meet legal, business, or contractual requirements?
- How are the logs reviewed, and by whom?
- Is automated reporting or alarming set up and effective?
- Is there ongoing evidence of active log review, such as a sign-off process?
- Are logs rotated or destroyed on a regular basis?
- Who has access to logs?
- Do logs contain sensitive information such as passwords, keys, or data that should not be exposed via logs to avoid data leakage?

Policies and procedures for log management should be documented and aligned to standards. ISO 27001 and ISO 27002 both provide basic guidance on logging, and NIST provide guidance in publication SP 800-92, “Guide to Computer Security Log Management.”

Since logging is driven by business needs, infrastructure and system design, and the organization’s functional and security requirements, specific organizational practices and standards need to be created and their implementation regularly assessed.

OWASP Logging Cheat Sheet the OWASP Logging Cheat Sheet available at:

https://www.owasp.org/index.php/Logging_Cheat_Sheet

The Cheat Sheet provides guidance on building application logging mechanisms, with an emphasis on security logging. This Logging Cheat Sheet is meant to be used to overcome the frequent problem that application event logging is overlooked or insufficient for comprehensive security.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 177, 812, and p. 565). Wiley. Kindle Edition.
- https://doi.org/10.6028/NIST.SP.800-92
- https://www.owasp.org/index.php/Logging_Cheat_Sheet

MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE (AI) BASED TOOLS

The emerging themes of emerging technologies present challenges for the proper protection of data. A few of the emerging technologies are cloud computing, the Internet of Things (IoT), machine learning, artificial intelligence (AI), and Big Data. Even thou this guide does not explore each of these topics in depth, the challenges they present to asset security and protecting the data have some common themes.

Note from Clement:

This is a new and emerging field. Even thou many vendors claim to have Machine Learning and AI being used within their products; it is still in its infancy. Below you have a bit more details than needed for the exam, but I am trying to give you a wider view and clearer picture.

AI as a wider definition includes machine learning and deep learning

Artificial intelligence and machine learning are the part of computer science that are correlated with each other. These two technologies are the most trending technologies which are used for creating intelligent systems.

Although these are two related technologies and sometimes people use them as a synonym for each other, but still, both are the two different terms in various cases.

On a broad level, we can differentiate both AI and ML as:

AI is a bigger concept to create intelligent machines that can simulate human thinking capability and behavior, whereas, machine learning is an application or subset of AI that allows machines to learn from data without being programmed explicitly.

Artificial Intelligence

Artificial intelligence is a field of computer science which makes a computer system that can mimic human intelligence. It is comprised of two words "**Artificial**" and "**intelligence**", which means "a human-made thinking power." Hence, we can define it as,

Artificial intelligence is a technology used to create intelligent systems that can simulate human intelligence.

The Artificial intelligence system does not require to be pre-programmed, instead of that, they use such algorithms which can work with their own intelligence. It involves machine learning algorithms such as Reinforcement learning algorithm and deep learning neural networks. AI is being used in multiple places such as Siri, Google AlphaGo, AI in Chess playing, etc.

Based on capabilities, AI can be classified into three types:

- **Weak AI**
- **General AI**
- **Strong AI**

Currently, we are working with weak AI and general AI. The future of AI is Strong AI.

Machine learning

At its simplest level, machine learning is defined as “the ability (for computers) to learn without being explicitly programmed.” Using mathematical techniques across huge datasets, machine learning algorithms essentially build models of behaviors and use those models as a basis for making future predictions based on new input data. It is Netflix offering up new TV series based on your previous viewing history, and the self-driving car learning about road conditions from a near-miss with a pedestrian.

Machine learning is about extracting knowledge from the data. It can be defined as *a subfield of artificial intelligence, which enables machines to learn from past data or experiences without being explicitly programmed.*

Machine learning enables a computer system to make predictions or take some decisions using historical data without being explicitly programmed. Machine learning uses a massive amount of structured and semi-structured data so that a machine learning model can generate accurate result or give predictions based on that data.

Machine learning works on algorithm which learn by its own using historical data. It works only for specific domains such as if we are creating a machine learning model to detect pictures of dogs, it will only give result for dog images, but if we provide a new data like cat image then it will become unresponsive. Machine learning is being used in various places such as for online recommender system, for Google search algorithms, Email spam filter, Facebook Auto friend tagging suggestion, etc.

It can be divided into three types:

- Supervised learning
- Reinforcement learning
- Unsupervised learning

Key differences between Artificial Intelligence (AI) and Machine learning (ML):

Artificial Intelligence	**Machine learning**
Artificial intelligence is a technology which enables a machine to simulate human behavior.	Machine learning is a subset of AI which allows a machine to automatically learn from past data without programming explicitly.
The goal of AI is to make a smart computer system like humans to solve complex problems.	The goal of ML is to allow machines to learn from data so that they can give accurate output.
In AI, we make intelligent systems to perform any task like a human.	In ML, we teach machines with data to perform a particular task and give an accurate result.
Machine learning and deep learning are the two main subsets of AI.	Deep learning is a main subset of machine learning.
AI has a very wide range of scope.	Machine learning has a limited scope.
AI is working to create an intelligent system which can perform various complex tasks.	Machine learning is working to create machines that can perform only those specific tasks for which they are trained.
AI system is concerned about maximizing the chances of success.	Machine learning is mainly concerned about accuracy and patterns.
The main applications of AI are **Siri, customer support using catboats**, Expert System, Online game playing, intelligent humanoid robot, etc.	The main applications of machine learning are **Online recommender system**, **Google search algorithms**, **Facebook auto friend tagging suggestions**, etc.
On the basis of capabilities, AI can be divided into three types, which are, **Weak AI**, **General AI**,	Machine learning can also be divided into mainly three types that are **Supervised learning**, **Unsupervised**

and **Strong AI**.	**learning**, and **Reinforcement learning**.
It includes learning, reasoning, and self-correction.	It includes learning and self-correction when introduced with new data.
AI completely deals with Structured, semi-structured, and unstructured data.	Machine learning deals with Structured and semi-structured data.

AI for cybersecurity

What benefits does artificial intelligence (AI) present for cybersecurity? AI's capability to analyze massive quantities of data with lightning speed means security threats can be detected in real time, or even predicted based on risk modeling. As AI reaches new frontiers, there must be a framework for ensuring AI is accurate and ethical.

Machine Learning in Information Security

So, what are the machine learning applications in information security?

In principle, machine learning can help businesses better analyze threats and respond to attacks and security incidents. It could also help to automate more menial tasks previously carried out by stretched and sometimes under-skilled security teams.

Subsequently, machine learning in security is a fast-growing trend. Analysts at ABI Research estimate that machine learning in cybersecurity will boost spending in big data, artificial intelligence (AI) and analytics to $96 billion by 2021, while some of the world's technology giants are already taking a stand to better protect their own customers.

Google is using machine learning to analyze threats against mobile endpoints running on Android - as well as identifying and removing malware from infected handsets, while cloud infrastructure giant Amazon has acquired start-up harvest.AI and launched Macie, a service that uses machine learning to uncover, sort and classify data stored on the S3 cloud storage service.

Simultaneously, enterprise security vendors have been working towards incorporating machine learning into new and old products, largely in a bid to improve malware detection. "Most of the major companies in security have moved from a purely "signature-based" system of a few years ago used to detect malware, to a machine learning system that tries to interpret actions and events and learns from a variety of sources what is safe and what is not," says Jack Gold, president and principal analyst at J. Gold Associates.

“It’s still a nascent field, but it is clearly the way to go in the future. Artificial intelligence and machine learning will dramatically change how security is done.”

Though this transformation will not happen overnight, machine learning is already emerging in certain areas. “**AI - has a wider definition which includes machine learning and deep learning**. It is in its early phase of empowering cyber defense where we mostly see the obvious use cases of identifying patterns of malicious activities whether on the endpoint, network, fraud or at the SIEM,” says Dudu Mimran, CTO of Deutsche Telekom Innovation Laboratories (and also of the Cyber Security Research Center at Israel’s Ben-Gurion University). “I believe we will see more and more use cases, in the areas of defense against service disruptions, attribution and user behavior modification.”

Here, we break down the top use cases of machine learning in security.

1. Using machine learning to detect malicious activity and stop attacks

Machine learning algorithms will help businesses to detect malicious activity faster and stop attacks before they get started. David Palmer should know. As director of technology at UK-based start-up Darktrace – a firm that has seen a lot of success around its machine learning-based Enterprise Immune Solution since the firm’s foundation in 2013 – he has seen the impact on such technologies.

Palmer says that Darktrace recently helped one casino in North America when its algorithms detected a data exfiltration attack that used a “connected fish tank as the entryway into the network.” The firm also claims to have prevented a similar attack during the Wannacry ransomware crisis last summer.

“Our algorithms spotted the attack within seconds in one NHS agency’s network, and the threat was mitigated without causing any damage to that organization,” he said of the ransomware, which infected more than 200,000 victims across 150 countries. “In fact, none of our customers were harmed by the WannaCry attack including those that hadn’t patched against it.”

2. Using machine learning to analyze mobile endpoints

Machine learning is already going mainstream on mobile devices, but thus far most of this activity has been for driving improved voice-based experiences on the likes of Google Now, Apple’s Siri, and Amazon’s Alexa. Yet there is an application for security too. As mentioned above, Google is using machine learning to analyze threats against mobile endpoints, while enterprise is seeing an opportunity to protect the growing number of bring-your-own and choose-your-own mobile devices.

In October, MobileIron and Zimperium announced a collaboration to help enterprises adopt mobile anti-malware solutions incorporating machine learning. MobileIron said it would integrate Zimperium’s machine learning-based threat detection with MobileIron’s security and compliance engine and sell the combined solution, which would address challenges like detecting device, network, and application threats and immediately take automated actions to protect the company's data.

Other vendors are looking to bolster their mobile solutions, too. Along with Zimperium, LookOut, Skycure (which has been acquired by Symantec), and Wandera are seen to be the leaders in the mobile threat detection and defense market. Each uses its own machine learning algorithm to detect potential threats. Wandera, for example, recently publicly released its threat detection engine MI: RIAM, which reportedly detected more than 400 strains of repackaged SLocker ransomware targeting businesses' mobile fleets.

3. Using machine learning to enhance human analysis

At the heart of machine learning in security, there is the belief that it helps human analysts with all aspects of the job, including detecting malicious attacks, analyzing the network, endpoint protection and vulnerability assessment. There is arguably most excitement though around threat intelligence.

For example, in 2016, MIT's Computer Science and Artificial Intelligence Lab (CSAIL) developed a system called AI^2, an adaptive machine learning security platform that helped analysts find those 'needles in the haystack'. Reviewing millions of logins each day, the system was able to filter data and pass it onto the human analyst, reducing alerts down to around 100 per day. The experiment – carried by CSAIL and start-up PatternEx — showed that the attack detection rate rose to 85 percent with a five-fold decrease in false positives.

4. Using machine learning to automate repetitive security tasks

The real benefit of machine learning is that it could automate repetitive tasks, enabling staff to focus on more important work. Palmer says that machine learning ultimately should aim to "remove the need for humans to do repetitive, low-value decision-making activity, like triaging threat intelligence. "Let the machines handle the repetitive work and the tactical firefighting like interrupting ransomware so that the humans can free up time to deal with strategic issues — like modernizing off Windows XP — instead."

Booz Allen Hamilton has gone down this route, reportedly using AI tools to more efficiently allocate human security resources, triaging threats so workers could focus on the most critical attacks.

5. Using machine learning to close zero-day vulnerabilities

Some believe that machine learning could help close vulnerabilities, particularly zero-day threats and others that target largely unsecured IoT devices. There has been proactive work in this area: A team at Arizona State University used machine learning to monitor traffic on the dark web to identify data relating to zero-day exploits, according to Forbes. Armed with this type of insight, organizations could potentially close vulnerabilities and stop patch exploits before they result in a data breach.

Hype and misunderstanding muddy the landscape

However, machine learning is no silver bullet, not least for an industry still experimenting with these technologies in proof of concepts. There are numerous pitfalls. Machine learning systems sometimes report false positives (from unsupervised learning systems where the algorithms infer categories based on data), while some analysts have spoken candidly about how machine learning in security can represent a "black box" solution, where CISOs aren't totally sure what's "under the hood." They are thus forced to place their trust and responsibility on the shoulders of the vendor – and the machines.

This idea of trust is not ideal in a world where some security solutions may not even be doing machine learning, after all. "Most of the machine learning inventions that have been touted aren't really doing any learning 'on the job' within the customer's environment," said Palmer. "Instead, they have models trained on malware samples in a vendor's cloud and are downloaded to customer businesses like antivirus signatures. This isn't particularly progressive in terms of customer security and remains fundamentally backward-looking."

Furthermore, on these training data samples — required for the algorithms to learn their models before being use in the 'real' world — there is the suggestion that poor data and implementation will result in even poorer results. "Machine learning is only as good as the input information you provide it (garbage in, garbage out)," says Gold. "So, if your machine learning algorithms are not well designed, the results won't be especially useful. Having algorithms that work on training data sets in the lab is one thing, but one of the biggest challenges around machine learning cyber defense is getting it working at scale in live, complex networks."

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 173). Wiley. Kindle Edition.
- https://www.mdsny.com/5-top-machine-learning-use-cases-for-security/
- https://www.javatpoint.com/difference-between-artificial-intelligence-and-machine-learning

MEDIA PROTECTION TECHNIQUES

This is NOT a new topic. It is well covered in most study book and standard such as NIST 800-88r1 has a lot of details on what are the requirement as far as marking, protection, transportation, sanitizing, and detection. So, we will keep this one short.

First, we must clarify the term media. It would include media of different format or legacy media such as formats, such as hard-copy documents, photos, and microfilm. It could also (more likely) be in reference to a wide range of digital formats, such as external hard drives, floppy disks, diskettes, magnetic tape cassettes, memory cards, flash drives, and optical (CD and DVD-ROM) disks.

Protection for the organization’s resources (hardware, software, personnel, intellectual property, and so on) is discussed thoroughly throughout the CBK. This section specifically addresses protection measures for media (material that carries data) and how to effectively manage those medias.

Managing media includes properly marking, protecting, transporting, sanitizing, and destroying media at the end of its life.

The goals for doing these activities, as stated in ISO 27002, are to “prevent unauthorized disclosure, modification, removal or destruction of information stored on media.”

This goes back to the CIA Triad; the organization doesn’t want unauthorized people to see what is on the organization’s media, and the organization wants the data stored on media to be accurate and available when needed.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 647). Wiley. Kindle Edition.
- NIST Sanitizing of media at https://Fnvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf&usg=AOvVaw1ri4RgwGKHUm4qr_uilECN

MICROSERVICES

This is NOT a new topic, the latest study reference from ISC2 has a lot of content related to Microservices. I will cover them briefly and you can consult your study book for more details.

Microservices are a popular form of service-oriented architecture that focus on delivering specific-purpose business capabilities as independently deployed services.

Microservices are small and focused software with minimal dependencies that have fast and short development times. Typically, they come with an immutable architecture. Microservices have a minimal commitment to specific technologies or software stacks. The orchestration of multiple microservices can be complex. With more microservices comes more complexity. Because each microservices endpoint is a specific delivery of business capability, each would have its own deployment, access management, and security concerns. Each of these concerns comes with challenges particular to it.

Evaluating the security of a microservices architecture requires taking a layered approach. The reason for this is that a microservices architecture is an information technology ecosystem in and of itself. Authentication and authorization from callers to services and transitively carrying the authentication/authorization (AuthN/AuthZ) across services is a necessary aspect of evaluating a microservices architecture. Evaluating the network security is another layer of a complete approach to microservices security. The microservices endpoints should not be exposed to public networks, particularly not the Internet. Check to make sure that there is an intermediary API that fields and filters all public calls to the microservices and that the microservices are in a controlled isolation from public networks. A firewall should enforce granular access control to each of the microservices' endpoints.

Microservices Architecture

Microservices architecture refers to a technique that gives modern developers a way to design highly scalable, flexible applications by decomposing the application into discrete services that implement specific business functions. These services, often referred to as "loosely coupled," can then be built, deployed, and scaled independently.

Each service communicates with other services, through standardized application programming interfaces (APIs), enabling the services to be written in different languages or on different technologies. This differs completely from systems built as monolithic structures where services were inextricably interlinked and could only be scaled together.

As each service has a limited functionality, it is much smaller in size and complexity. The term microservice comes from this discrete functionality design, not from its physical size.

Why a microservices architecture?

Microservices architecture has risen in popularity because its modular characteristics lead to flexibility, scalability, and reduced development effort. Its deployment flexibility, and the rise of cloud-native serverless and function-as-a-service deployment options (such as AWS Lambda and Microsoft Azure Cloud Functions), have created the perfect environment for microservices to flourish in today's IT landscape.

These cloud platforms enable microservices and functions to be scaled from inactivity to high volume and back again while customers pay only for the compute capacity they use.

As businesses are continuously looking to be more agile, reduce bottlenecks, and improve application delivery times, microservices architecture continues to rise in popularity.

Benefits of a Microservices Architecture

- Application components can be built in different programming languages
- Individual continuous development and deployment streams can be sustained
- Extremely scalable applications can be built
- Use of cloud-native function-as-a-service deployment options is possible
- Lower operational costs often result
- Isolation and loose coupling enable compartmentalized upgrades and enhancements

Example Microservices Architecture Use Cases

1. **Adopt cloud-native deployment options:** leverage serverless and function-as-a-service for more efficient and scalable operations.
2. **Migrate functionality from legacy applications:** decompose services from large monolithic applications so they can be independently maintained and scaled.
3. **Leverage modern application architecture:** embrace event-driven, loosely coupled microservice application patterns, with the ability to leverage different programming languages depending on use case needs. For example, go for computationally heavy functions, Node.js for quick web apps, etc.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 743). Wiley. Kindle Edition.
- **https://www.tibco.com/reference-center/what-is-microservices-architecture?utm_medium=cpc&utm_source=google&utm_content=s&utm_campaign=ggl_s_en_nam_TCI_nonbrand_events_beta&utm_term=%2Bwhat%20%2Bare%20%2Bmicroservices&_bt=473116235440&_bm=b&_bn=g&gclid=Cj0KCQjw9_mDBhCGARIsAN3PaFOas-57CzQagUL9Vv2m1BPu_YdNmEFdZrIYFQt5YnUKTB5U9ieoyaoaAoMCEALw_wcB**

MICRO-SEGMENTATION

This is a category that was added within the new CBK under Domain 4 – Telecommunication and Network Security. It is listed at 4.1 under the heading “Assess and implement secure design principles in network architectures”

Most people are aware of Segmentation and Segregation, but it is no longer enough in today’s cloud environment and you must go one step further. See more details further down discussing traditional segmentation versus micro-segmentation.

Micro segmentation is a method of creating zones in data centers and cloud environments to isolate workloads from one another and secure them individually. With micro segmentation, system administrators can create policies that limit network traffic between workloads based on a Zero Trust approach. Organizations use micro segmentation to reduce the network attack surface, improve breach containment and strengthen regulatory compliance.

Micro segmentation and software-defined networking (SDN) are related but separate concepts, so it’s important to understand the distinction. SDN virtualizes network functionality by separating the control and data planes and implementing the network intelligence in software. While micro-segmentation can be implemented with traditional networking technology, SDN-enabled micro-segmentation is far more flexible because it enables system administrators to define and manage security entirely through software. For this and other reasons, a growing number of security and network virtualization vendors are partnering joint solutions for micro-segmentation.

Beyond Traditional Segmentation

Network segmentation – dividing the network into subnets of related components – has been widely adopted by security architects as a response to increasingly sophisticated cyberattacks that regularly breach the network perimeter. By preventing threats from performing lateral movement and privilege escalation, network segmentation limits the damage breaches can cause and streamlines mitigation activities.

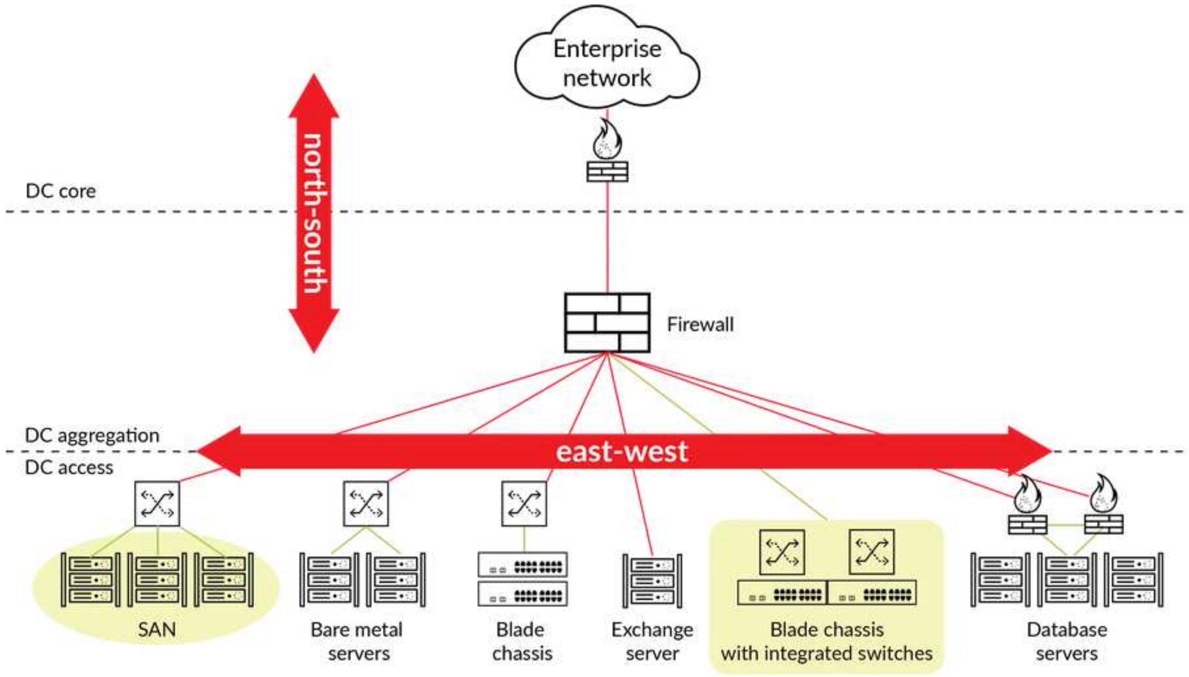
Traditional segmentation works best on “north-south” traffic – that is, client-server interactions that cross the security perimeter. Today’s hybrid cloud architectures have all but obliterated the importance of the perimeter because most traffic flows east-west (server to server) between applications (see graphic on the page below).

In addition, the proliferation of virtual machines means a single server can host hundreds of workloads, each with its own security requirements. Such environments require more granular security, right down to the workload level. That is what micro-segmentation is all about.

How Micro-segmentation Works

Micro-segmentation helps provide consistent security across data centers and hybrid cloud platforms alike by virtue of three key principles: visibility, granular security and dynamic adaptation.

Unlike north-south communications, east-west traffic is usually not subject to firewall inspection and is, for all practical purposes, invisible to the network security team. To be effective, micro-segmentation requires visibility into all network traffic. While there are several ways to monitor traffic, the hypervisor touches every packet on the network and is therefore uniquely positioned to provide the necessary visibility.



Granular security means network administrators can strengthen and pinpoint security by creating specific policies for overly sensitive workloads. The goal is to prevent lateral movement of threats with policies that precisely control traffic in and out of specific workloads, such as weekly payroll runs or updates to human resource databases.

Dynamic adaptation ensures these protections remain in place as workloads move around in today’s highly dynamic environments. In micro-segmentation, security policies are expressed in terms of abstract concepts such as application tiers rather than network constructs such as IP addresses and port numbers. Changes to the application or infrastructure trigger automatic revisions to security policies in real time, requiring no human intervention.

Benefits of Micro-segmentation

Organizations that adopt micro-segmentation realize tangible benefits in the form of a reduced attack surface, improved breach containment, stronger compliance posture and streamlined policy management.[1] More specifically:

- **Reduced attack surface:** Micro-segmentation provides visibility into the complete network environment without slowing development or innovation. Application developers can integrate security policy definition early in the development cycle and ensure that neither application deployments nor updates create new attack vectors. This is particularly important in the fast-moving world of DevOps.
- **Improved breach containment:** Micro-segmentation gives security teams the ability to monitor network traffic against predefined policies as well as shorten the time to respond to and remediate breaches.
- **Stronger regulatory compliance:** Using micro-segmentation, regulatory officers can create policies that isolate systems subject to regulations from the rest of the infrastructure. Granular control of communications with regulated systems reduces the risk of noncompliant usage.
- **Streamlined policy management:** Moving to a micro-segmentation architecture provides an opportunity to simplify the management of firewall policies. An emerging best practice is to use a single consolidated policy for subnet access control as well as threat detection and mitigation, rather than performing these functions in different parts of the network. This approach reduces the attack surface and strengthens the organization's security posture.

Use Cases

The range of use cases for micro-segmentation is vast and growing. Here are some representative examples:

- **Development and production systems:** In the best-case scenario, organizations carefully separate development and test environments from production systems. However, these measures may not prevent careless activity, such as developers taking customer information from production databases for testing. Micro-segmentation can enforce a more disciplined separation by granularly limiting connections between the two environments.

- **Security for soft assets:** Companies have a huge financial and reputational incentive to protect "soft" assets, such as confidential customer and employee information, intellectual property, and company financial data. Micro-segmentation adds another level of security to guard against exfiltration and malicious actions that can cause downtime and interfere with business operations.
- **Hybrid cloud management:** Micro-segmentation can provide seamless protection for applications that span multiple clouds and implement uniform security policies across hybrid environments composed of multiple data centers and cloud service providers.
- **Incident response:** As noted earlier, micro-segmentation limits lateral movement of threats and the impact of breaches. In addition, micro-segmentation solutions provide log information to help incident response teams better understand attack tactics and telemetry to help pinpoint policy violations to specific applications.

There are a series of topics related to micro-segmentation, they are defined one by one as their own topic within this study guide. See them within the document above and below. Topics include:

- Software-Defined Wide Area Network (SD-WAN)
- Software Defined Networks (SDN)
- Virtual eXtensible Local Area Network (VXLAN)
- Encapsulation

Source:

- https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation
- https://www.guardicore.com/micro-segmentation/benefits-micro-segmentation/
- The definitive guide to micro-segmentation at: https://cdn2.hubspot.net/hubfs/407749/Downloads/Illumio_eBook_The_Definitive_Guide_to_Micro_Segmentation_2017_08.pdf

PERFORM CONFIGURATION MANAGEMENT (CM)

(e.g., provisioning, baselining, automation)

This is a topic that was already covered within most study books for the CISSP, it is now listed within Domain 7 Security Operations under the heading 7.3. So, this section will be brief, and you can refer to your study book for a lot more details.

Configuration management is the sum of the activities used to protect the totality of an IT system by controlling its configurations. This begins with the secure configuration of an IT system when it is first built. Once the system is in the production environment, it needs to be monitored to control any changes to its configuration.

The organization also needs a formal process for requesting, reviewing, and approving changes to the approved configuration. Having a configuration management capability is important for several reasons.

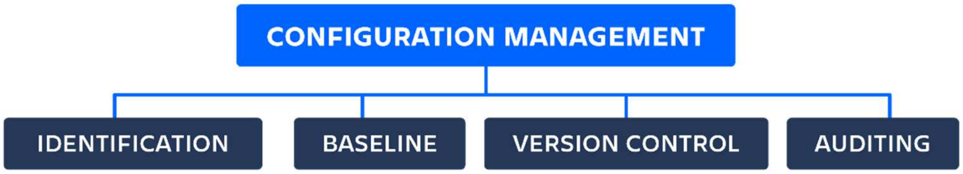
First, configuration management has perhaps the largest and most direct impact on an IT system's security posture. In addition, IT vendors' default settings are often unsafe. One simple misconfiguration, such as leaving a guest account open, can bypass all other security controls.

Second, even when a system is secured with the right configuration when it is first built, subsequent software installs can undo configuration settings or allow users to change them, intentionally or otherwise.

Lastly, configuration management helps with other security domains. In disaster recovery management, for example, having defined configurations for IT components helps you restore your systems to a secure state faster.

During the 1950s the United States Department of Defense developed a technical management discipline to track changes in the development of complex systems. It gave this system and various iterations very technical names, until in 2001 it published a consolidated guidebook that established the technical management system now called configuration management. Today, configuration management is not only used by the defense department, but in software development, IT service management, civil engineering, industrial engineering, and more.

What is configuration management?



CONFIGURATION MANAGEMENT

IDENTIFICATION

BASELINE

VERSION CONTROL

AUDITING

Configuration management is a system engineering process for establishing consistency of a product's attributes throughout its life. In the technology world, configuration management is an IT management process that tracks individual configuration items of an IT system. IT systems are composed of IT assets that vary in granularity. An IT asset may represent a piece of software, or a server, or a cluster of servers. The following focuses on configuration management as it directly applies to IT software assets and software asset CI/CD.

Software configuration management is a system engineering process that tracks and monitors changes to a software systems configuration metadata. In software development, configuration management is commonly used alongside version control and CI/CD infrastructure. This post focuses on its modern application and use in agile CI/CD software environments.

Why is configuration management important?

Configuration management helps engineering teams build robust and stable systems using tools that automatically manage and monitor updates to configuration data. Complex software systems are composed of components that differ in granularity of size and complexity. For a more concrete example consider a micro-service architecture. Each service in a microservice architecture uses configuration metadata to register itself and initialize. Some examples of software configuration metadata are:

- Specifications of computational hardware resource allocations for CPU, RAM, etc.
- Endpoints that specify external connections to other services, databases, or domains
- Secrets like passwords and encryption keys

It is easy for these configuration values to become an afterthought, leading to the configuration to become disorganized and scattered. Imagine numerous post-it notes with passwords and URLs blowing around an office. Configuration management solves this challenge by creating a "source of truth" with a central location for configuration.

Git is a fantastic platform for managing configuration data. Moving configuration data into a Git repository enables version control and the repository to act as a source of truth. Version control also solves another configuration problem: unexpected breaking changes. Managing unexpected changes using code review and version control helps to minimize downtime.

Configuration values will often be added, removed, or modified. Without version control this can cause problems. One team member may tweak a hardware allocation value so that the software runs more efficiently on their personal laptop. When the software is later deployed to a production environment, this new configuration may have a suboptimal effect or may break.

Version control and configuration management solve this problem by adding visibility to configuration modifications. When a change is made to configuration data, the version control system tracks it, which allows team members to review an audit trail of modifications.

Configuration version control enables rollback or "undo" functionality to configuration, which helps avoid unexpected breakage. Version control applied to the configuration can be rapidly reverted to a last known stable state.

How configuration management fits with DevOps, CI/CD and agile

Configuration data has historically been hard to wrangle and can easily become an afterthought. It's not really code so it's not immediately put in version control and it's not first-class data, so It isn't stored in a primary database. Traditional and small-scale system administration is usually done with a collection of scripts and ad-hoc processes. Configuration data can be overlooked at times, but it is critical to system operation.

The rise of cloud infrastructures has led to the development and adoption of new patterns of infrastructure management. Complex, cloud-based system architectures are managed and deployed using configuration data files. These new cloud platforms allow teams to specify the hardware resources and network connections they need provisioned through human and machine-readable data files like YAML. The data files are then read, and the infrastructure is provisioned in the cloud. This pattern is called infrastructure as code (IaC).

DevOps configuration management

In the early years of internet application development, hardware resources and systems administration were primarily performed manually. System administrators wrangled configuration data while manually provisioning and managing hardware resources based on configuration data.

DevOps configuration is the evolution and automation of the systems administration role, bringing automation to infrastructure management and deployment.

DevOps configuration also brings system administration responsibility under the umbrella of software engineering. Enterprises today utilize it to empower software engineers to request and provision needed resources on demand. This removes a potential organizational dependency bottleneck of a software development team waiting for resources from a separate system administration team.

CI/CD configuration management

CI/CD configuration management utilizes pull request-based code review workflows to automate deployment of code changes to a live software system. This same flow can be applied to configuration changes. CI/CD can be set up so that approved configuration change requests can immediately be deployed to a running system.

Agile configuration management

Configuration management enables agile teams to clearly triage and prioritize configuration work. Examples of configuration work are chores and tasks like:

- Update the production SSL certificates
- Add a new database endpoint
- Change the password for dev, staging, and production email services.
- Add API keys for a new third-party integration

Once a configuration management platform is in place, teams have visibility into the work required for configuration tasks. Configuration management work can be identified as dependencies for other work and properly addressed as part of agile sprints.

Configuration management tools

Git

Git is the industry-leading version control system to track code changes. Adding configuration management data alongside code in a Git repository provides a holistic version control view of an entire project. Git is a foundational tool in higher-level configuration management. The following list of other configuration management tools is designed to be stored in a Git repository and leverage Git version control tracking.

Docker

Docker introduced containerization that is an advanced form of configuration management -- like a configuration lockdown. Docker is based on configuration files called Dockerfiles, which contain a list of commands that are evaluated to reconstruct the expected snapshot of operating system state. Docker creates containers from these Dockerfiles that are snapshots of a preconfigured application. Dockerfiles are committed to a Git repository for version tracking and need additional configuration management to deploy them to infrastructure.

Terraform

Terraform is an open source configuration management platform by HasiCorp. Terraform uses IaC to provision and manage clusters, cloud infrastructure, or services. Terraform supports Amazon Web Services (AWS), Microsoft Azure, and other cloud platforms. Each cloud platform has its own representation and interface for common infrastructure components like servers, databases, and queues. Terraform built an abstraction layer of configuration tools for cloud platforms that enable teams to write files that are reproducible definitions of their infrastructure.

Ansible, Salt Stack, Chef, Puppet

Ansible, Salt Stack, and Chef are IT automation frameworks. These frameworks automate many traditional system administrators' processes. Each framework uses a series of configuration data files -- usually YAML or XML -- that are evaluated by an executable.

The configuration data files specify a sequence of actions to take to configure a system. The actions are then run by the executable. The executable differs in language between the systems -- Ansible and Salt Stack are Python based and Chef is Ruby. This workflow is similar to running ad-hoc shell scripts but offers a more structured and refined experience through the respective platform's ecosystems. These tools are what will bring enable the automation needed to achieve CI/CD.

How to implement configuration management

Identification

The first action towards configuration management is information gathering. Configuration data should be aggregated and compiled from different application environments, development, staging, and production for all the components and services in use. Any secret data like passwords and keys should be identified and securely encrypted and stored. At this point configuration data should be organized into data files that can be pointed to as a central source of truth.

Baseline

After configuration data has been aggregated and organized a baseline can be established. A baseline configuration is a known state of configuration that will successfully operate the dependent software without error. This baseline is usually created by reviewing the configuration of a functioning production environment and committing those configuration settings.

Version Control

Your development project should use a version control system. If not, install Git, initialize a repository for the project, and add the configuration data files to the repository. A word of caution before adding configuration data to a repository: make sure that any secret data like passwords or keys are encrypted with an external key. Secret data accidentally committed to a repository is a huge risk. It needs to be scrubbed from the repositories history or it will be at risk of being exploited.

Auditing

Having configuration data organized and added to a repository enables collaboration and visibility into the system's configuration. The popular pull request workflow that software teams use to review and edit code can then be applied to configuration data files. This helps build out an audit and accounting system. Any changes applied to the configuration must be reviewed and accepted by the team. This adds accountability and visibility into configuration changes.

In conclusion…

Configuration management is a necessary tool for managing complex software systems. Lack of configuration management can cause serious problems with reliability, uptime, and the ability to scale a system. Many current software development tools have configuration management features built in. Bitbucket offers a powerful system for configuration management that is built around Git pull request workflows and CI/CD pipelines.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 635). Wiley. Kindle Edition.
- https://www.upguard.com/blog/5-configuration-management-boss
- https://www.atlassian.com/continuous-delivery/principles/configuration-management

PRIVACY BY DESIGN (PbD)

This is a topic under Domain 3 – Security Architecture and Engineering, it is under 3.1 Research, implement and manage engineering processes using secure design principles. This topic fall with some of the regulations such as GDPR and also within the best practices regarding privacy.

The **General Data Protection Regulation** (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). Under GDPR) controllers are required to integrate privacy expectations and controls into the development processes for applications and systems. This concept, **privacy by design**, is extended through the concept of **privacy by default**. When an individual is being given a choice about which information is to be gathered, the default choice should be the option that provides the highest level of privacy to the individual.

The 7 Foundational Principles of Privacy by Design

These information management principles and the philosophy and methodology they express can apply to specific technologies, business operations, physical architectures and networked infrastructure entire information ecosystems.

The universal principles of the **Fair Information Practices (FIPs)** are affirmed by those of **Privacy by Design (PbD)** but go beyond them to seek the highest global standard possible. Extending beyond Fair Information Practices, Privacy by Design represents a significant "raising" of the bar in the area of privacy protection.

1. Proactive not Reactive; Preventative not Remedial

The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred − it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

Whether applied to information technologies, organizational practices, physical design, or networked information ecosystems, Privacy by Design begins with an explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently (for example, preventing (internal) data breaches from happening in the first place). This implies:

- A clear commitment, at the highest levels, to set and enforce high standards of privacy generally higher than the standards set out by global laws and regulation.
- A privacy commitment that is demonstrably shared throughout by user communities and stakeholders, in a culture of continuous improvement.

- Established methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive, systematic, and innovative ways.

2. Privacy as the Default Setting

We can all be certain of one thing − the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy it is built into the system, by default.

This Privacy by Design principle, which could be viewed as Privacy by Default, is particularly informed by the following FIPs:

- Purpose Specification – the purposes for which personal information is collected, used, retained and disclosed shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.
- Collection Limitation – the collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.
- Data Minimization − the collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.
- Use, Retention, and Disclosure Limitation – the use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.
- Where the need or use of personal information is not clear, there shall be a presumption of privacy and the precautionary principle shall apply: the default settings shall be the most privacy protective.

3. Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

Privacy must be embedded into technologies, operations, and information architectures in a holistic, integrative and creative way. Holistic, because additional, broader contexts must always be considered. Integrative, because all stakeholders and interests should be consulted. Creative, because embedding privacy sometimes means re-inventing existing choices because the alternatives are unacceptable.

- A systemic, principled approach to embedding privacy should be adopted, one that relies upon accepted standards and frameworks, which are amenable to external reviews and audits. All fair information practices should be applied with equal rigor, at every step in the design and operation.
- Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy risks and all measures taken to mitigate those risks, including consideration of alternatives and the selection of metrics.
- The privacy impacts of the resulting technology, operation or information architecture, and their uses, should be demonstrably minimized, and not easily degraded through use, misconfiguration or error.

4. Full Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made.

Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.

Privacy by Design does not simply involve the making of declarations and commitments − it relates to satisfying all of the organization’s legitimate objectives, not only its privacy goals. Privacy by Design is doubly enabling in nature, permitting full functionality − real, practical results and beneficial outcomes to be achieved for multiple parties.

- When embedding privacy into a given technology, process, or system, it should be done in such a way that full functionality is not impaired, and to the greatest extent possible, that all requirements are optimized.
- Privacy is often positioned in a zero-sum manner as having to compete with other legitimate interests, design objectives, and technical capabilities, in a given domain. Privacy by Design rejects taking such an approach. It embraces legitimate non-privacy objectives and accommodates them, in an innovative positive-sum manner.
- All interests and objectives must be clearly documented, desired functions articulated, metrics agreed upon and applied, and trade-offs rejected as often being unnecessary, in favor of finding a solution that enables multi-functionality.
- Additional recognition is garnered for creativity and innovation in achieving all

objectives and functionalities in an integrative, positive-sum manner. Entities that succeed in overcoming outmoded zero-sum choices are demonstrating first-class global privacy leadership, having achieved the Gold Standard.

5. End-to-End Security – Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

Privacy must be continuously protected across the entire domain and throughout the life cycle of the data in question. There should be no gaps in either protection or accountability. The "Security" principle has special relevance here because, at its essence, without strong security, there can be no privacy.

- Security Entities must assume responsibility for the security of personal information (generally commensurate with the degree of sensitivity) throughout its entire lifecycle, consistent with standards that have been developed by recognized standards development bodies.
- Applied security standards must assure the confidentiality, integrity and availability of personal data throughout its lifecycle including, inter alia, methods of secure destruction, appropriate encryption, and strong access control and logging methods.

6. Visibility and Transparency – Keep it Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify!

Visibility and transparency are essential to establishing accountability and trust. This Pricacy by Design (PbD) principle tracks well to Fair Information Practices in their entirety, but for auditing purposes, special emphasis may be placed upon the following FIPs:

- Accountability – The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured.
- Openness – Openness and transparency are key to accountability. Information about

the policies and practices relating to the management of personal information shall be made readily available to individuals.

- Compliance – Complaint and redress mechanisms should be established, and information communicated about them to individuals, including how to access the next level of appeal. Necessary steps to monitor, evaluate, and verify compliance with privacy policies and procedures should be taken.

7. Respect for User Privacy – Keep it User-Centric

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric!

The best Privacy by Design results are usually those that are consciously designed around the interests and needs of individual users, who have the greatest vested interest in the management of their own personal data. Empowering data subjects to play an active role in the management of their own data may be the single most effective check against abuses and misuses of privacy and personal data. Respect for User Privacy is supported by the following FIPs:

- Consent – The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.
- Accuracy – personal information shall be as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.
- Access – Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
- Compliance – Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal.
- Respect for User Privacy goes beyond these FIPs and extends to the need for human-machine interfaces to be human-centered, user-centric and user-friendly so that informed privacy decisions may be reliably exercised. Similarly, business operations and physical architectures should also demonstrate the same degree of consideration for the individual, who should feature prominently at the center of operations involving collections of personal data.

Source:

- https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 43). Wiley. Kindle Edition.
- Cavoukian, Ann, Ph.D., Information & Privacy Commissioner, Ontario, Canada. Creation of a Global Privacy Standard (November 2006), at:

  www.ipc.on.ca/images/Resources/gps.pdf

PRIVILEGE ESCALATION

(e.g., managed service accounts, use of sudo, minimizing its use)

Privilege escalation is an attack vector that many businesses face due to loss of focus on permission levels. As a result, security controls are not sufficient to prevent a privilege escalation.

Privilege escalation attacks occur when a threat actor gains access to an employee's account, bypasses the proper authorization channel, and successfully grants themselves access to data they are not supposed to have. When deploying these attacks threat actors are typically attempting to exfiltrate data, disrupt business functions, or create backdoors.

All these actions can have a major impact on business continuity and should be considered when drafting a business continuity plan.

When encounter a privilege escalation attack, how you respond is critical. Here are a few questions to consider:

- What did the attacker have permission and access to?
- How are business services currently being impacted?
- What other activities were performed on this account during the duration of the attack?

What are the types of Privilege Escalation attacks?

Not every attack will provide threat actors with full access to the targeted system. In these cases, a privilege escalation is required to achieve the desired outcome. There are two types of privilege escalation attacks including vertical and horizontal.

Vertical Privilege Escalation

Vertical privilege escalation occurs when an attacker gains access directly to an account with the intent to perform actions as that person. This type of attack is easier to pull off since there is no desire to elevate permissions. The goal here is to access an account to further spread an attack or access data the user has permissions to.

Day in and day out I analyze numerous phishing emails that attempt to perform this attack. Whether it is a "bank", "Amazon", or any other countless number of ecommerce sites, the attack is the same. "*Your account will be deactivated due to inactivity. Please click this link and login to keep your account active."* This is, however, one example of many cookie-cutter phishing templates seen in "the wild".

Horizontal Privilege Escalation

Horizontal privilege escalation is a bit tricky to pull off as it requires the attacker to gain access to the account credentials as well as elevating the permissions. This type of attack tends to require a deep understanding of the vulnerabilities that affect certain operating systems or the use of hacking tools.

Phishing campaigns have been used to perform the first part of the attack to gain access to the account. When it comes to elevating permissions, the attacker has a few options to choose from. One option is to exploit vulnerabilities in the operating system to gain system or root-level access. The next option would be to use hacking tools, like Metasploit, to make the job a bit easier.

How To Prevent A Privilege Escalation Attack

Unfortunately, users are the weakest link in the security chain. With just a single click, they could compromise a system or network. To mitigate this risk, businesses implement security awareness programs along with a methodology for validating the effectiveness of the training. In most cases, phishing simulation software, like KnowBe4, GoPhish, or Phishme can adequately train users to identify phishing email attempts.

Privilege escalation, like other cyber-attacks, takes advantage of system and process vulnerabilities. In order to prevent these attacks, consider implementing proper processes for patch management, new software development/implementation, and user account modification requests as well as an automated tool to monitor for such changes.

Implementing these processes will give you the proper safeguards in place to prevent or deter and attacker from attempting privilege escalation. Finally, an intrusion detection system (IDS) and/or intrusion prevention system (IPS) provides an additional layer of security to derail attempts at escalating privileges.

New exploits are being created daily and it is our responsibility to ensure we protect ourselves from the attack. A proper patch management process will help ensure all systems and applications are current with the latest patches.

During the quest for new and improved software, we must not forget to include security in the process. Oftentimes, security is set aside to meet the business or client needs. Software code reviews or vendor management processes will help keep security in the loop and strengthen your development practices.

Example of Privilege Escalation using sudo

A flaw was found within the UNIX/Linux sudo utility allowing root privileges for any local user. The Sudo privilege escalation vulnerability was discovered by security researchers from Qualys.

According to Qualys researchers, the issue is a heap-based buffer overflow exploitable by any local user (normal users and system users, listed in the sudoers file or not), with attackers not being required to know the user's password to successfully exploit the flaw.

Source:

- https://purplesec.us/privilege-escalation-attacks/
- https://www.bleepingcomputer.com/news/security/new-linux-sudo-flaw-lets-local-users-gain-root-privileges/

PROGRAMMING LANGUAGE
(In software Security Controls in software development)

This is not a new topic. It is something that was already within most study books and we will only scratch the surface of this topic. For the exam, you must know the different language type such as Compiled versus Interpreted. You must understand the difference between the two when it comes to security. See a quick overview below:

Programming languages are the means by which correlated sets of instructions are written to produce programs that can be executed by a computer.

Programming language grammar consists of symbols that describe different data types, methods to create and manipulate data, and logical structures that can control the flow of execution of the program.

Language Types

There are two types of software languages: compiled and interpreted.

Each language type has security implications for the software that it is used to produce.

Compiled

Compiled languages are those where the program instructions are translated into a form that is directly interpretable by the machine. A program called a compiler does this translation. An advantage of compiled languages is that the compiler is typically optimized for the target hardware. And because of this translation into a machine code, compiled languages typically execute faster than interpreted languages.

Compiled languages have many features that support security. The compilation process checks the program structure for correctness. A security type system can be employed at compile time to enforce information flows to verify or report violations of confidentiality or integrity.

It is possible to generate a certificate during compilation as a form of proof that the source code was compiled following a set of rules that satisfies a security policy.

Interpreted

An interpreted programming language is one where most of its code is executed directly without first having to compile it into machine-language instructions. Many developers favor interpreted languages for how quickly they can be used to write programs. Many are easy to learn and powerful.

There are potential security trade-offs with the speed and facility that come with using an interpreted language. Interpreted languages do not come with the up-front benefits of program correctness, type checking, and security policy verification that compiled languages do.

Securing interpreted languages requires layering extra efforts to the development done in the interpreted language, including automated and comprehensive testing, scanning, security testing, and code reviews.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 722). Wiley. Kindle Edition.
- https://kb.iu.edu/d/agsz
- https://www.freecodecamp.org/news/compiled-versus-interpreted-languages/

PROVISION RESOURCES SECURELY

This section includes Asset Inventory, Asset Management, and Configuration Management.

Just like many other topics, this one is not new within the CBK, but it was renamed slightly in the latest CBK. It used to be called Securely Provision Resources. It is about Provisioning Resources through configuration management.

Secure provisioning of IT resources has many important elements. Some of these are covered within 1.12 Apply Supply Chain Risk Management (SCRM) concepts of Domain 1. This topic addresses asset inventory and configuration management. Configuration management is already covered as a separate section within the study guide.

Asset Inventory

Fundamental to any sort of a change, control, or configuration management system and its success will begin with an inventory of hardware and software. Now doing an inventory of all the hardware is a way of identifying what is present, what is and should be and what is and should not be included in this. And the same is true of software. We are looking to identify what software is present, the vendor, the licenses, and this is done for a couple of reasons. One is so that we know what we have, and two so that we know what our license posture is to be sure we are not at risk for operating unlicensed software, which means it essentially is not part of our normal inventory, and perhaps it's not licensed or being paid for.

Now having developed inventories of both hardware and software, we want to employ a configuration management process. Now, to break this down, configuration management is a discipline for evaluating, coordinating, approving or disapproving, and implementing the changes to artifacts used to construct and maintain software systems. Now to compare configuration management with change control, the easiest way to remember is change management, or change control, is more of a macrolevel institutional or organizational level process, whereby change is identified, analyzed, and then in some controlled way, introduced into the organization if it is found that that is beneficial. Configuration management would be more of a microlevel process, by which we break the changes down into smaller and smaller pieces to implement into the various components within the organization.

The assets that we place under configuration management will, of course, be of a variety of kinds. Some will be physical, some will be virtual, some will be cloud, perhaps, if cloud computing is part of your operation, and then, of course, we have the applications.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 632). Wiley. Kindle Edition.
- https://www.youtube.com/watch?v=m44JAPliw1g
- https://www.youtube.com/watch?v=n2wQ70Urfc8

QUANTUM COMPUTING

Quantum computers could spur the development of new breakthroughs in science, medications to save lives, machine learning methods to diagnose illnesses sooner, materials to make more efficient devices and structures, financial strategies to live well in retirement, and algorithms to quickly direct resources such as ambulances.

To understand quantum computing, it is useful to first think about conventional computing. We take modern digital computers and their ability to perform a multitude of different applications for granted. Our desktop PCs, laptops and smart phones can run spreadsheets, stream live video, allow us to chat with people on the other side of the world, and immerse us in realistic 3D environments. But at their core, all digital computers have something in common. They all perform simple arithmetic operations. Their power comes from the immense speed at which they can do this. Computers perform billions of operations per second. These operations are performed so quickly that they allow us to run extraordinarily complex high-level applications.

Although there are many tasks that conventional computers are particularly good at, there are still some areas where calculations seem to be exceedingly difficult. Examples of these areas are: Image recognition, natural language (getting a computer to understand what we mean if we speak to it using our own language rather than a programming language), and tasks where a computer must learn from experience to become better at a particular task. Even though there has been much effort and research poured into this field over the past few decades, our progress in this area has been slow and the prototypes that we do have working usually require very large supercomputers to run them, consuming a vast quantity of space and power.

We can ask the question: Is there a different way of designing computing systems, from the ground up? If we could start again from scratch and do something completely different, to be better at these tasks that conventional computers find hard, how would we go about building a new type of computer?

A new kind of computing

Quantum computing is radically different from the conventional approach of transforming bits strings from one set of 0's and 1's to another. With quantum computing, everything changes. The physics that we use to understand bits of information and the devices that manipulate them are totally different. The way in which we build such devices is different, requiring new materials, new design rules and new processor architectures. Finally, the way we program these systems is entirely different. This document will explore the first of these issues, how replacing the conventional bit (0 or 1) with a new type of information - the qubit - can change the way we think about computing.

Instead of bits, which conventional computers use, a quantum computer uses quantum bits—known as qubits. To illustrate the difference, imagine a sphere. A bit can be at either of the two poles of the sphere, but a qubit can exist at any point on the sphere. So, this means that a computer using qubits can store an enormous amount of information and uses less energy doing so than a classical computer. By entering this quantum area of computing where the traditional laws of physics no longer apply, we will be able to create processors that are significantly faster (a million or more times) than the ones we use today. Sounds fantastic, but the challenge is that quantum computing is also incredibly complex.

The pressure is on the computer industry to find ways to make computing more efficient, since we reached the limits of energy efficiency using classical methods. By 2040, according to a report by the Semiconductor Industry Association, we will no longer have the capability to power all of the machines around the world. That is precisely why the computer industry is racing to make quantum computers work on a commercial scale. No small feat, but one that will pay extraordinary dividends.

Source:

- https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/
- https://www.forbes.com/sites/bernardmarr/2017/07/04/what-is-quantum-computing-a-super-easy-explanation-for-anyone/

RANSOMWARE

Ransomware is a type of malware designed to extort victims for financial gain. Once activated, ransomware prevents users from interacting with their files, applications or systems until a ransom is paid, usually in the form of an untraceable currency like Bitcoin. In some cases, the victim is instructed to pay the perpetrator by a set time or risk losing access forever. In other cases, the perpetrator intermittently raises the ransom demands until the victim pays.

Ransomware infections are common and costly. According to security research firm CyberSecurity Ventures, by 2021, a business will fall victim to a ransomware attack every 11 seconds and global annual ransomware damage costs will reach $20 billion. While ransomware impacts businesses and institutions of every size and type, attackers often target large enterprises and governments with deeper pockets.

Because ransomware attacks are carried out by cybercriminals, most law enforcement agencies and security experts discourage ransom payments. According to the FBI, paying ransom does not guarantee you will regain access to your encrypted data. Some victims who pay ransom never receive decryption keys. Some are extorted for additional money after the initial ransom is paid. Even worse, some victims who pay ransom are attacked again in the future by the same criminal.

Ransomware is Continuously Evolving

Ransomware has evolved significantly over the years. Early “computer locker” attacks would lock up a computer by disabling keyboard or mouse functionality. In most cases, you could simply ignore ransom demands and restore the computer to its previous working state using off-the-shelf malware removal tools.

Today’s ransomware sophisticated and invasive. They can spread quickly throughout an organization, incapacitating users and disrupting business operations. Some ransomware programs go a step further, initiating distributed denial of service attacks. All platforms are affected by this, including Windows endpoints, Windows servers and even Macs. Others steal confidential data or compromising information and threaten to release it publicly.

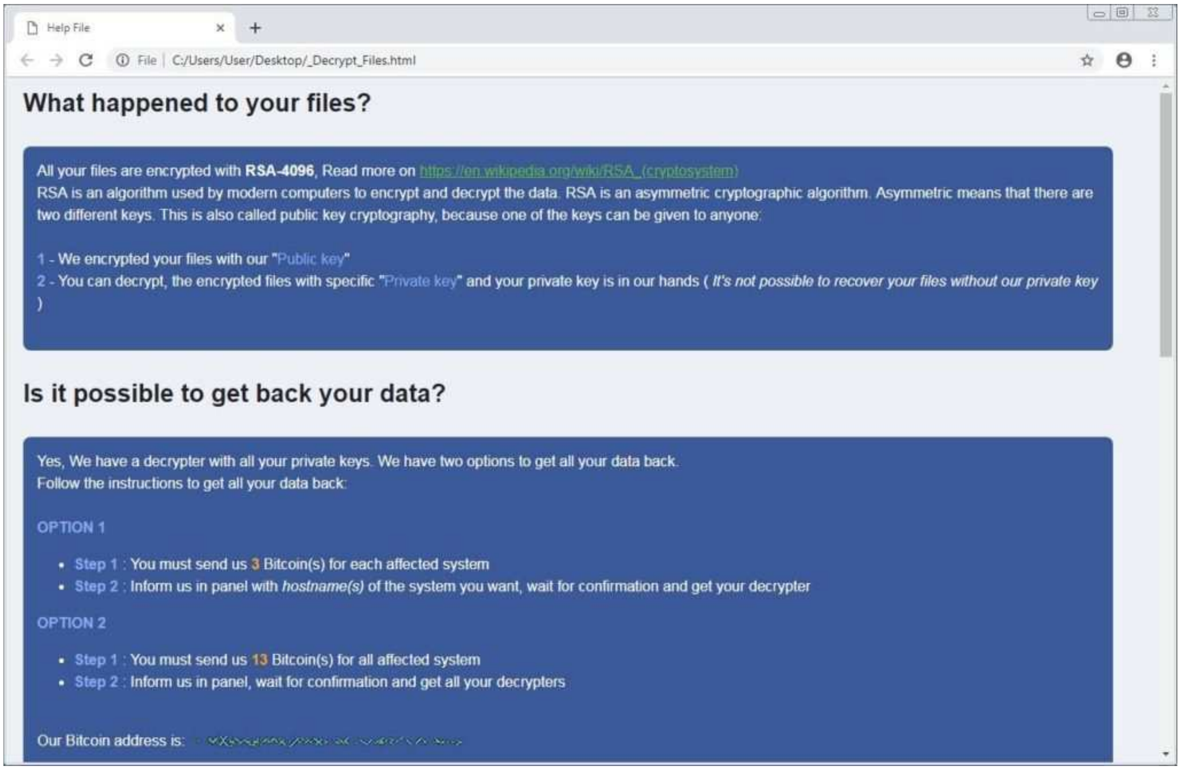
Some examples of noteworthy ransomware attacks in recent years include:

- The 2017 NotPetya attack irreversibly encrypted the master boot records of computers running the Windows operating system. It is said to have caused more than $10 billion in damages worldwide. The attack hobbled global enterprises like Merck, Maersk and FedEx, which attributed a $300 million loss to the incident.
- The 2017 WannaCry cryptoworm outbreak infected over 200,000 computers in over 150 countries, wreaking havoc on organizations like Britain’s National Health Service, which was forced to close critical healthcare facilities, cancel surgeries and turn away patients for days. By one estimate, the total economic impact of the WannaCry attack was $4

billion.

- The 2019 RobbinHood attack crippled the city of Baltimore's IT services for almost a month, disabling email, voicemail, a parking fines database and a system used to pay water bills, property taxes and vehicle citations.

Example of a Ransom note, this one is from the RobbinHood ransomware.



What happened to your files?

All your files are encrypted with **RSA-4096**, Read more on https://en.wikipedia.org/wiki/RSA_(cryptosystem)
RSA is an algorithm used by modern computers to encrypt and decrypt the data. RSA is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone:

1 - We encrypted your files with our "Public key"
2 - You can decrypt, the encrypted files with specific "Private key" and your private key is in our hands (*It's not possible to recover your files without our private key*)

Is it possible to get back your data?

Yes, We have a decrypter with all your private keys. We have two options to get all your data back.
Follow the instructions to get all your data back:

OPTION 1

- Step 1 : You must send us 3 Bitcoin(s) for each affected system
- Step 2 : Inform us in panel with *hostname(s)* of the system you want, wait for confirmation and get your decrypter

OPTION 2

- Step 1 : You must send us 13 Bitcoin(s) for all affected system
- Step 2 : Inform us in panel, wait for confirmation and get all your decrypters

Our Bitcoin address is: [redacted]

Avoiding and Mitigating Ransomware Attacks

Security experts recommend the following:

- Routinely back up all enterprise servers and PCs. While data backups can't prevent ransomware, you can use them to recover from certain types of ransomware attacks. Many experts recommend backing up data to the cloud to protect against sophisticated ransomware attacks that identify and destroy or encrypt local backup files.
- Use anti-virus and endpoint detection and response tools to block (blacklist) known ransomware variants at the point of entry.
- Remove local administrator rights from standard user accounts to reduce attack surfaces and prevent the spread of ransomware throughout an organization, since some ransomware attacks attempt to gain local admin rights to inflict damage.
- Use application greylisting to proactively defend against previously unknown ransomware variants. With a greylisting approach, you can restrict read, write and

modify permissions for unknown applications to prevent ransomware from encrypting data. You can also use greylisting to block access to network drives to prevent ransomware attacks from propagating across the enterprise.

What is greylisting: Greylisting is a powerful Anti-Spam technology that is used to detect if the sending server of a message is **RFC compliant**. This is done through temporarily blocking unknown senders and caching details of the initial message.

Source:

- https://www.cyberark.com/what-is/ransomware/

REDUNDANT / BACKUP POWER

This item was added to the latest CBK. However, it is not a new topic. You must be familiar with power related issues as well as the different solution that exist to minimize the impact of power failure. UPS and Generators are coming to mind here. You must understand the advantage and disadvantages of each and when they are best used.

Redundant or Backup power is one topic that has been in the news more than every within the past 12 months. We had power blackout in California due to forest fire. More recently, we had major power failure in Texas due to extreme cold weather. Thus, the need to plan for and have redundant power source.

This is all part of "Hardening the infrastructure" which is decreasing the likelihood that a compromise will occur may lead to developing a more disaster-resilient infrastructure. Implementing high availability environments such as system clusters, private clouds, mirrored systems working in conjunction with environmental redundancy such as **backup power supplies, redundant electrical generation,** and HVAC systems will decrease the likelihood of system failure. Beyond supporting the individual information systems, the environmental redundancies may also speed recovery of the business processes.

We will talk at high-level about Uninterruptable Power Supply (UPS) and the different types.

What is a UPS?

Put simply, a UPS is a device that:

- Provides backup power when utility power fails, either long enough for critical equipment to shut down gracefully so that no data is lost or corrupted, or long enough to keep required loads operational until a generator comes online.
- It also conditions incoming power so that all-too-common sags and surges don't damage sensitive electronic gear.

  No company can afford to leave its IT assets unprotected from power issues. Here are just a few of the reasons why:

- Even short outages can be trouble. Losing power for as little as a quarter second can trigger events that may keep IT equipment unavailable for anywhere from 15 minutes to many hours. And downtime is costly.

- Utility power is not always clean. By law, electrical power can vary widely enough to cause significant problems for IT equipment. According to current U.S. standards, for example, voltage can legally vary from 5.7 percent to 8.3 percent under absolute specifications.

- Utility power is not 100 percent reliable. In the U.S., in fact, it is only 99.9 percent reliable, which translates into a likely nine hours of utility outages every year.

- The problems and risks are intensifying. Today's storage systems, servers and network devices use components so miniaturized that they falter and fail under power conditions earlier-generation equipment easily withstood.

- Generators and surge suppressors are not enough. Generators can keep systems operational during a utility outage, but they take time to startup and provide no protection from power spikes and other electrical disturbances. Surge suppressors help with power spikes but not with issues like power loss, under-voltage and brownout conditions.

- Availability is everything these days. Once, IT played a supporting role in the enterprise. These days it is absolutely central to how most companies compete and win. When IT systems are down, core business processes quickly come to a standstill.

An uninterruptible power supply (UPS), also known as battery backup, provides different levels of protection against power problems, depending on the UPS type: online, standby (offline), or line interactive.

Online UPS

The double-conversion online UPS provides the best level of power protection for critical applications.

Why? In contrast to the other two designs, an online UPS continually regenerates new, clean AC power through its continuous duty inverter and seamlessly operates on AC or DC (battery) power.

It also has several layers of protective circuits that further safeguard connected equipment and ensure it is always receiving **100% conditioned and regulated** AC power.

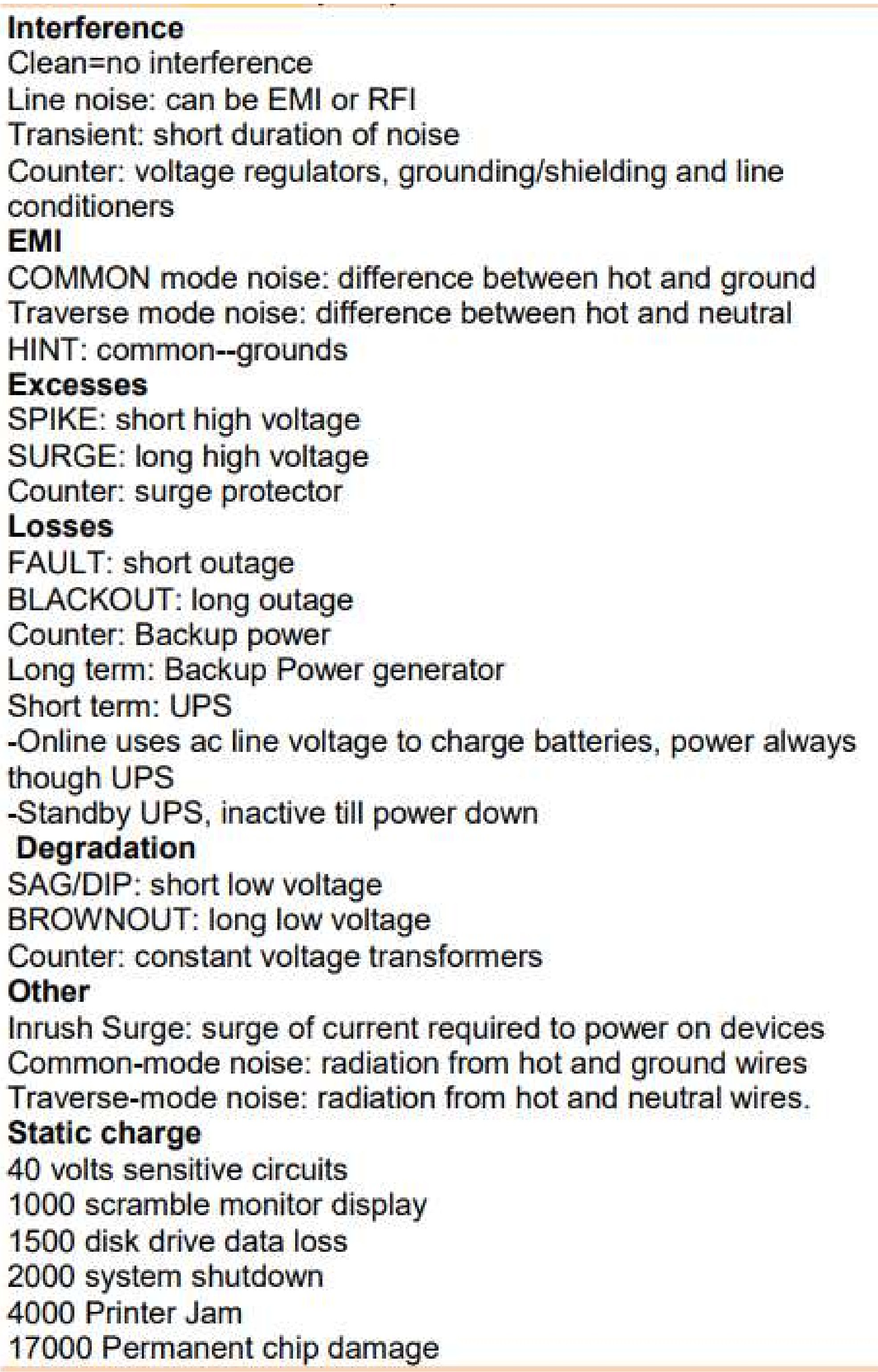
Additionally, an online UPS can provide long periods of battery runtime by adding extra battery packs.

Standby and Line-interactive

Standby and line-interactive UPSs turn on the inverter when the power fails and can only provide short periods of battery runtime (by design). This leads to an interruption (transfer time) when the inverter power takes over. Also, during normal operation, they leave equipment connected directly to the utility with very limited protection from common power disturbances. This may be acceptable for non-critical devices, but it **has a risk factor**. If an application cannot afford risks, the right solution is an online UPS.

COMMON POWER ISSUES:

See below an extract from the Sunflower Study Guide:



Interference
Clean=no interference
Line noise: can be EMI or RFI
Transient: short duration of noise
Counter: voltage regulators, grounding/shielding and line conditioners

EMI
COMMON mode noise: difference between hot and ground
Traverse mode noise: difference between hot and neutral
HINT: common--grounds

Excesses
SPIKE: short high voltage
SURGE: long high voltage
Counter: surge protector

Losses
FAULT: short outage
BLACKOUT: long outage
Counter: Backup power
Long term: Backup Power generator
Short term: UPS
-Online uses ac line voltage to charge batteries, power always though UPS
-Standby UPS, inactive till power down

Degradation
SAG/DIP: short low voltage
BROWNOUT: long low voltage
Counter: constant voltage transformers

Other
Inrush Surge: surge of current required to power on devices
Common-mode noise: radiation from hot and ground wires
Traverse-mode noise: radiation from hot and neutral wires.

Static charge
40 volts sensitive circuits
1000 scramble monitor display
1500 disk drive data loss
2000 system shutdown
4000 Printer Jam
17000 Permanent chip damage

Source

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 74). Wiley. Kindle Edition.
- https://www.falconups.com/ups-comparison-online-standby-line-interactive.htm
- https://www.ia.omron.com%2Fdata_pdf%2Fguide%2F572%2Fups_tg_e_1_1.pdf&usg=AOvVaw3YDRjDepefm8WZiobJ_YcZ
- Sunflower Study Guide https://www.sunflower-cissp.com/

REMEDIATION (generate test output and generate report)

Remediation within the CBK is in the context of Domain 6 - Security Assessments and Testing.

Remediation is part of the steps involve when dealing with and incident. The remediation phase marks the return from reduced to full functionality. The quick fix in the mitigation can often leave the system with no functionality or partial functionality. The final fix in the remediation phase often coincides with the return to full functionality. The remediation phase also includes those actions necessary to address damages resulting from the incident. This could be monetary fees/settlements paid to regulators/affected entities or efforts made to assuage/compensate those entities.

Remediation is an act of offering an improvement to replace a mistake and set it right. Often the presence of vulnerability in one area may indicate weakness in process or development practices that could have replicated or enabled similar vulnerability in other locations. Therefore, while remediating, it is important for the tester to carefully investigate the tested entity or applications with ineffective security controls in mind.

Because of these reasons, the respective company should take steps to remediate any exploitable vulnerability within a reasonable period of time after the original test. In fact, as soon as the company has completed these steps, the pen tester should perform a retest to validate the newly implemented controls which are capable to mitigate the original risk.

The remediation efforts extending for a longer period after the initial pen test possibly require performing a new testing engagement to ensure accurate results of the most current environment. This determination should be made after a risk analysis of how much change has occurred since the original testing was completed.

Moreover, in specific conditions, the flagged security problem may illustrate a basic flaw in respective environment or application. Therefore, the scope of a retest should consider whether any changes caused by remediation identified from the test are classified as significant. All changes should be retested; however, whether an entire system retest is necessary or not will be determined by the risk assessment of the changes.

Source:

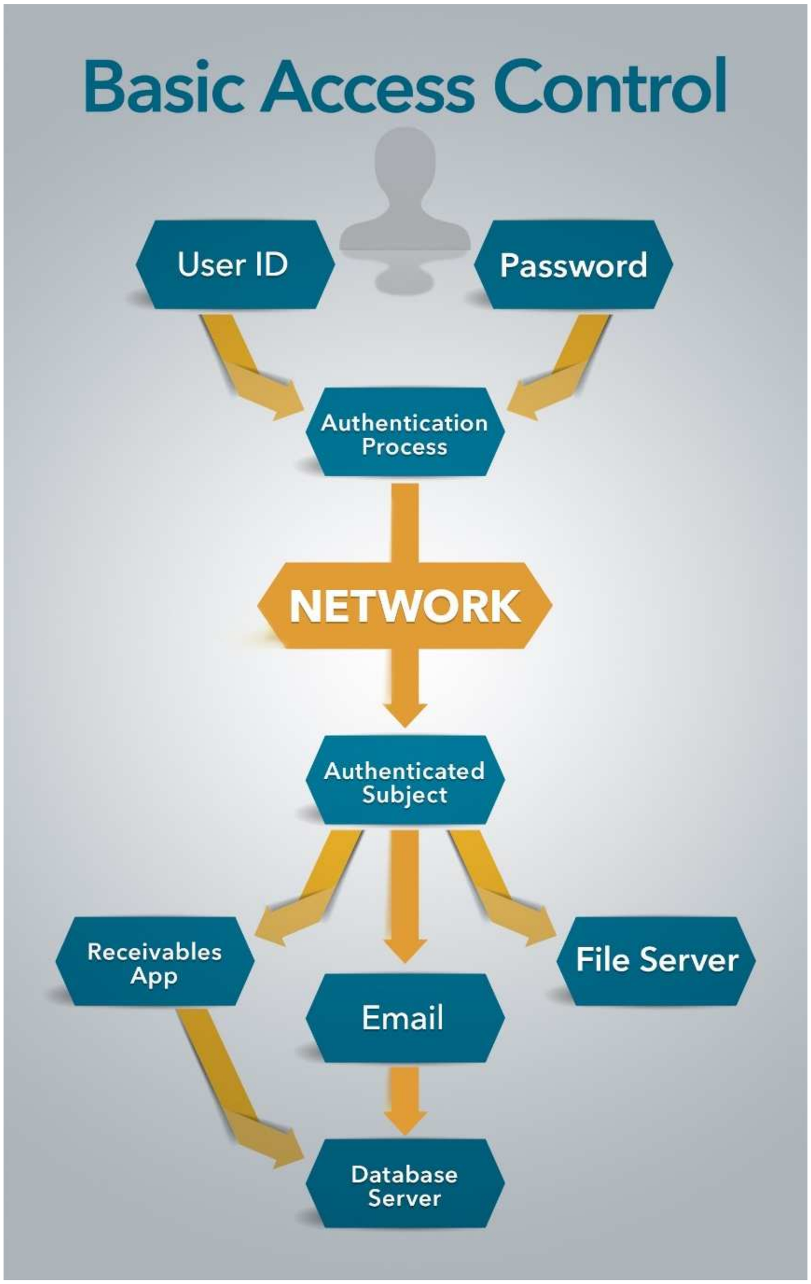
- https://www.tutorialspoint.com/penetration_testing/penetration_testing_legal_issues.htm
- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 661). Wiley. Kindle Edition.

RISK-BASED ACCESS CONTROL

Risk Based Access Control make use of authentication practices commensurate with associated risk, including ensuring the subject’s identity continues to be checked and confirmed; questionable situations require a new authentication.

Most organizations use two types of access control: basic and risk-based.

Figure 1 below shows the standard access control process.



Basic Access Control

In weak basic access control, the human subject uses a user ID and a single factor of authentication to verify identity. This an event providing access to the accounts receivable application, email, and file server as authorized by profiles, security groups, access control lists, etc. at a specific point in time.

The organization likely logs access to all resources and might have monitoring solutions to detect anomalous network or device behavior. However, the user subject behavior is not usually analyzed. When it is, security teams must react to alerts. Further, much behavior associated with account compromise is difficult to detect on mobile devices.

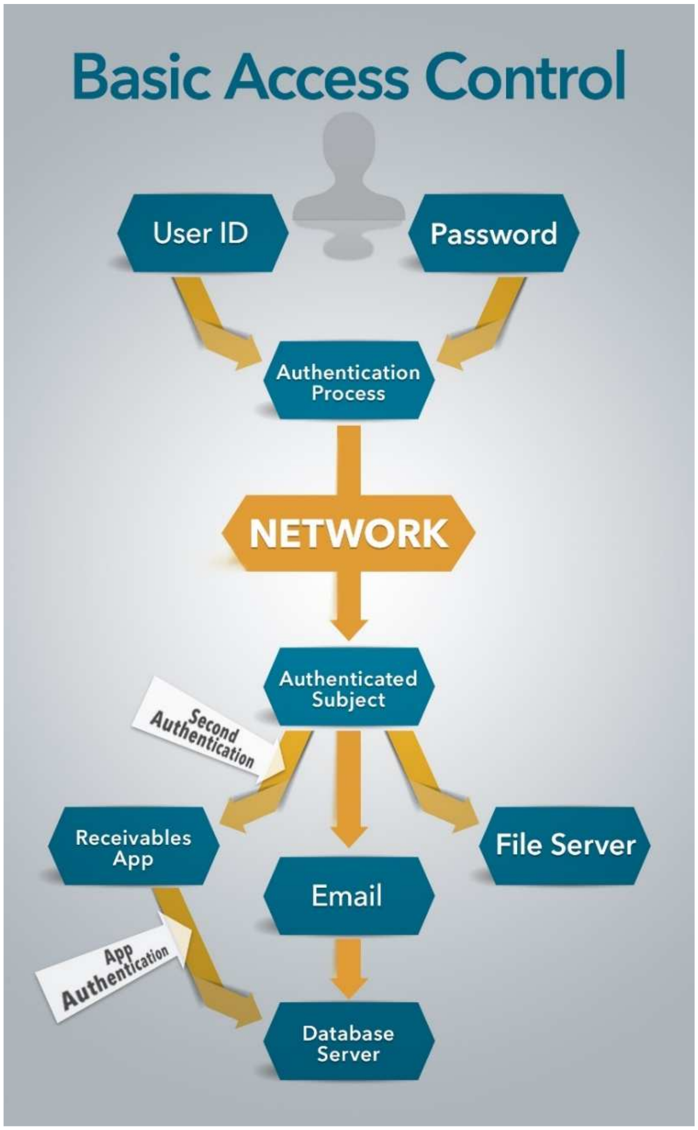
We can strengthen basic access control by adding a second authentication factor. Using multiple factors, known as strong authentication, significantly reduces identity verification risk, but it still only checks identity once.

Risk Based Access Control

Risk-based access control is traditionally implemented in roughly two ways: basic and strong.

A basic approach causes a user to log into the network for general access and then into additional resources considered high risk.

See the picture below:



In this example, the organization requires any user already authenticated to the network to authenticate again before accessing the receivables application. This helps ensure that someone accessing a user workstation is the person represented by the authenticated identity.

If a user walked away from her/his desk without locking the desktop, and someone else sat down at the keyboard, they would have to know the receivables password to access the high-risk resource. Unless, of course, the authorized user was already signed into the receivables app.

Strong risk-based access control might use additional device and user characteristics, including

- The role of the user
- The type and owner of the device used

- The time of access and the day of week
- What is being accessed
- What is being done with the data

While risk-based access control is better than standard access control—basic or strong—it still does not go far enough to address today's threats targeting all attack surfaces. We need to know throughout any session that the identity authenticated continues to be the person, application, or entity we expect.

Most organizations should be going beyond standard access control. Any one of the traditional authentication factors is not enough. Even if an organization uses multifactor authentication, attackers today are more than capable of taking control of machines. Once the attacker owns a machine, it is not a big jump to take over the user's account. We must be looking for this.

Risk-based access control is the direction in which organizations should be heading. Even without continuous authentication, use of session characteristics and user/device behavior monitoring is key to protecting the most sensitive information.

When combined with continuous authentication, risk-based access becomes a strong control for preventing, detecting, and immediately responding when levels of confidence in authenticated subjects fall below a threshold.

Source:

- https://www.toolbox.com/tech/devops/articles/risk-based-access-control-and-the-role-of-continuous-authentication/

ROLE DEFINITION (e.g., People assigned to new role)

This topic falls under Domain 5 – Identity and Access Management (IAM). Under paragraph 5.5 which is “Manage the identity and access provisioning lifecycle” you will find role definition.

Provisioning is the process of coordinating the creation of user accounts, e-mail authorizations in the form of **rules and roles**, and other tasks such as provisioning of physical resources associated with enabling new users.

Large organizations employ thousands of people with ever changing needs to access devices, applications and information. Most of the access requirements are driven by an individual's roles and responsibilities, which keep changing overtime due to promotions, shifts in geography and attrition. Organizations need to provision systems securely and efficiently and also de-activate them based on requirements.

Role based provisioning aims at providing a user access to specific data and applications based on his role. It is an automated selective process with varying levels of access provisions based on how senior or powerful the person's role in the organization is.

Your identity management should include a Workflow. A Workflow allows administrators to specify a sequence of events to add users based on the users' roles and the approval of others in the organization. The automated process ensures consistency and allows auditing of each step in the provisioning process.

It should also be noted that the provisioning process and other identity management operations should be the same system for all entity types. However, the way and extent that employees are provisioned will differ from customers and partners. Different system and different administration methods should not be required for different types of users.

Source:

- https://searchsecurity.techtarget.com/feature/Identity-and-Access-Management-Provisioning
- https://www.happiestminds.com/Insights/role-based-provisioning/

RUNTIME

This is a topic within Domain 8 – Software Development Security, it is under 8.2 “Identify and apply security controls in software development ecosystems”.

RTE which is the acronym for "Runtime Environment."

As soon as a software program is executed, it is in a runtime state. In this state, the program can send instructions to the computer's processor and access the computer's memory (RAM) and other system resources.

When software developers write programs, they need to test them in the runtime environment. Therefore, software development programs often include an RTE component that allows the programmer to test the program while it is running. This allows the program to be run in an environment where the programmer can track the instructions being processed by the program and debug any errors that may arise. If the program crashes, the RTE software keeps running and may provide important information about why the program crashed. When you see the name of a software program with the initials "RTE" after it, it usually means the software includes a runtime environment.

While developers use RTE software to build programs, RTE programs are available to everyday computer users as well. Software such as Adobe Flash Player and Microsoft PowerPoint Viewer allow Flash movies and PowerPoint presentations to be run within the player software. These programs provide a runtime environment for their respective file formats. The most common type of RTE, however, is the Java RTE (or JRE), which allows Java applets and applications to be run on any computer with JRE installed.

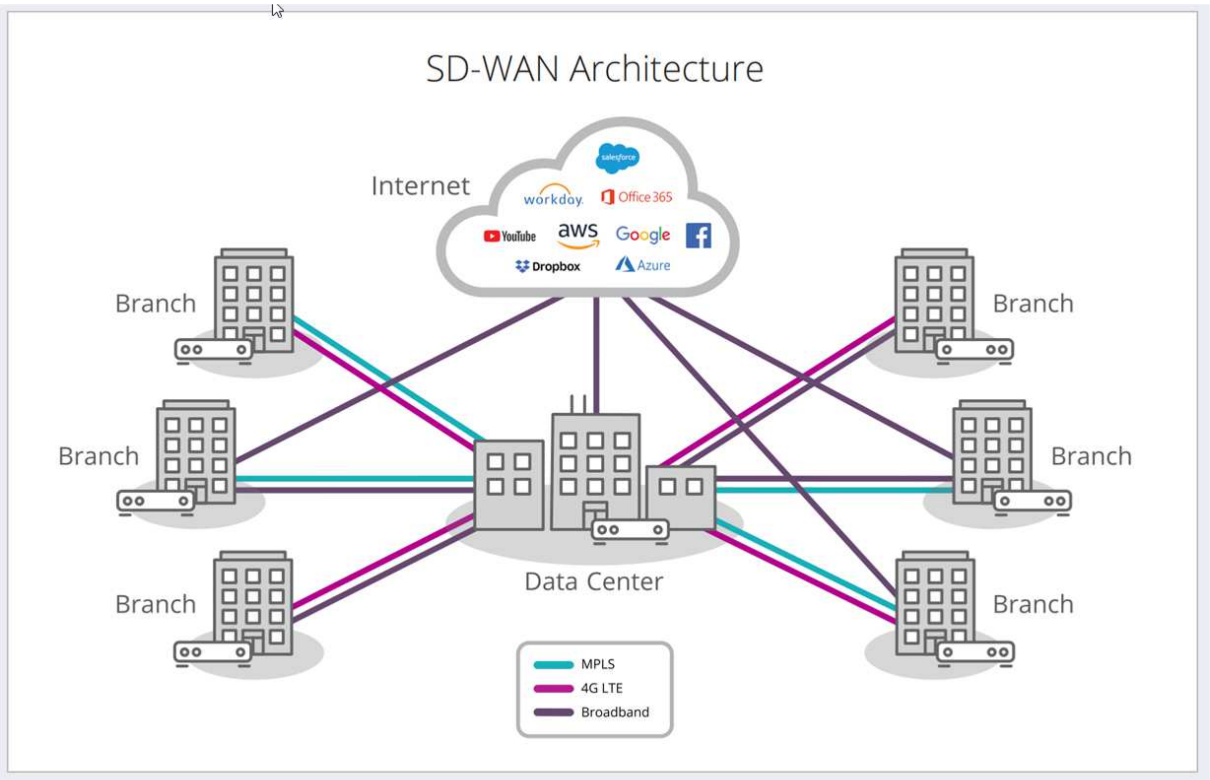
Source:

- https://techterms.com/definition/rte#

SOFTWARE DEFINED WIDE AREA NETWORK (SD-WAN)

NOTE FROM CLEMENT:
This is a topic related to Micro-segmentation.

A Software-defined Wide Area Network (SD-WAN) is a virtual WAN architecture that allows enterprises to leverage any combination of transport services – including MPLS, LTE and broadband internet services – to securely connect users to applications.



An SD-WAN uses a centralized control function to securely and intelligently direct traffic across the WAN. This increases application performance and delivers a high-quality user experience, resulting in increased business productivity, agility and reduced costs for IT.

Traditional WANs based on conventional routers were never designed for the cloud. They typically require backhauling all traffic – including cloud- destined traffic – from branch offices to a hub or headquarters data center where advanced security inspection services can be applied. The delay caused by backhaul impairs application performance resulting in a poor user experience and lost productivity.

Unlike the traditional router-centric WAN architecture, the SD-WAN model is designed to fully support applications hosted in on-premises data centers, public or private clouds and SaaS services such as Salesforce.com, Workday, Office 365 and Dropbox, while delivering the highest levels of application performance.

An SD-WAN enables cloud-first enterprises to deliver a superior application **Q**uality **o**f **EX**perience (QoEX) for users. Using intelligence and by identifying applications, an SD-WAN provides application-aware routing across the WAN. Each class of applications receives the appropriate QoS and security policy enforcement, all in accordance with business needs.

Secure local internet breakout of IaaS and SaaS application traffic from the branch provides the highest levels of cloud performance while protecting the enterprise from threats. Unlike SD-WAN, the conventional router-centric model distributes the control function across all devices in the network and simply routes traffic based on TCP/IP addresses and ACLs. This model tends to be rigid, inefficient and not cloud-friendly, resulting in a poor user experience.

Times have changed, and enterprises are using the cloud and subscribing to software-as-a-service (SaaS). While users traditionally connected back to the corporate data center to access business applications, they are now accessing those same applications in the cloud.

As a result, the traditional WAN is no longer suitable mainly because backhauling all traffic – including that destined to the cloud – from branch offices to the headquarters introduces latency and impairs application performance. SD-WAN provides WAN simplification, lower costs, bandwidth efficiency and a seamless on-ramp to the cloud with significant application performance especially for critical applications without sacrificing security and data privacy.

You can watch a nice overview of SD-Wan at https://youtu.be/5Tv-Lf8_3NM

Source:

- https://www.silver-peak.com/sd-wan/sd-wan-explained
- See a nice video at https://youtu.be/5Tv-Lf8_3NM

SERVERLESS

The term **serverless** refers to a cloud computing model where the cloud vendor owns the responsibility of provisioning, executing, and dynamically managing compute resources for the user, instead of the user owning the responsibility themselves.

Although the term incorrectly implies that no physical servers are involved, a serverless environment is one that abstracts away physical servers so that the end user need not be concerned with them.

One of the main benefits of serverless computing is that a user pays only for the compute resources consumed to execute a service in the cloud. For example, traditionally to run applications in the cloud, you would have to spin up several virtualized servers to meet capacity and pay for the usage even if your applications sit idle - wasting time and money. However, with serverless, the cloud vendor is responsible for ensuring that you use just the right compute resources to meet any demand.

Serverless computing simplifies the process of developing and deploying code. Applications and code can be developed to be completely serverless, or they can be written to work in conjunction with traditional apps.

Serverless databases remove the need to provision or scale database hardware. Additionally, a serverless architecture does not require any setup or maintenance - including scaling to demand - from your staff, because the cloud vendor takes care of these responsibilities.

Function as a Service (FaaS)

Function as a Service (**FaaS**) is a serverless type of cloud computing service that allows users to develop, run, and manage functionality of an application without having to provision and manage the underlying compute resources. Without having to manage servers and by only paying for what you need, you have the time and the resources to focus on your business and the application itself, rather than the infrastructure supporting it.

With FaaS you can do programming or upload modular pieces of functionality (or code) into the cloud that can be independently executed and without the hassle of having to manage your own server. This means developers can make changes to applications on the fly. Prior to FaaS, you would have to provision servers to handle an entire load but now scaling and provisioning are done automatically for you through the different functions (or pieces of code) that you deploy.

FaaS use cases mostly include on-demand services that can be shut down when not in use, saving you the cost of running a server continuously. Code is triggered by a user event (like someone clicking on a web page) which then calls other servers to execute the command.

Source:

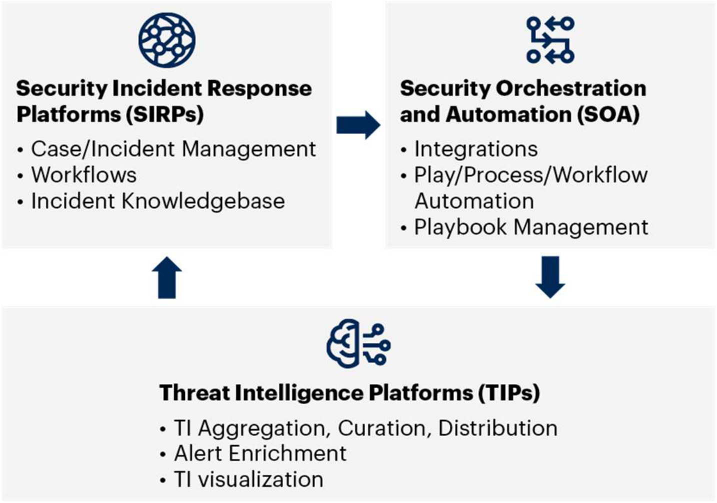
- https://www.tibco.com/reference-center/what-is-serverless
- https://www.tibco.com/reference-center/what-is-function-as-a-service

SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

The term was originally coined by Gartner. Gartner defines it as: SOAR refers to technologies that enable organizations to collect inputs monitored by the security operations team. For example, alerts from the SIEM system and other security technologies — where incident analysis and triage can be performed by leveraging a combination of human and machine power — help define, prioritize and drive standardized incident response activities. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.

SOAR is the convergence of 3 technologies together:

SOAR Convergence of Three Technologies (SIRP, SOA and TIP)



Security Incident Response Platforms (SIRPs)

- Case/Incident Management
- Workflows
- Incident Knowledgebase

Security Orchestration and Automation (SOA)

- Integrations
- Play/Process/Workflow Automation
- Playbook Management

Threat Intelligence Platforms (TIPs)

- TI Aggregation, Curation, Distribution
- Alert Enrichment
- TI visualization

Source: Gartner
727304_C

Gartner

Fireeye describe it as:

SOAR stands for Security Orchestration, Automation, and Response. The term is used to describe three software capabilities – threat and vulnerability management, security incident response and security operations automation. SOAR allows companies to collect threat-related data from a range of sources and automate responses to low-level threats.

Gartner who came out with the term, defined the three capabilities. **Threat and vulnerability management (Orchestration)** covers technologies that help amend cyber threats, while **Security Operations automation (Automation)** relates to the technologies that enable automation and orchestration within operations. As many the cyber threats facing companies will require multiple technologies to combat them and several team members to conduct manual tasks and liaise information, the orchestration of remediation must be seamless. While orchestration targets efficiency when executing threat remediation, automation aims to reduce the time of these actions using machine learning – making the orchestration process itself more efficient. **Security incident response (Response)** is how the response to a threat is planned, managed, coordinated and monitored. Response measures the process of responding to a threat or vulnerability and can be used to inform strategy.

SOAR systems can help define, prioritize and standardize functions that respond to cyber incidents. In other words, SOAR stacks enable organizations to determine the issues, define the solutions and then automate the response. The system is often adopted by organizations to improve efficiency, making security more self-operating. By removing the need for human assistance, threats and vulnerabilities can be responded to quicker and workers can better prioritize their time.

The software allows security teams to gain attacker insights with threat rules derived from insight into attacker **tactics, techniques and procedures (TTPs)** and **known indicators of compromise (IOC)s**. To do this it uses multiple threat intelligence feeds (organized and analyzed information on potential and current threats) which supplements threat detection.

Combat budget restraints

SOAR was introduced to combat a number of issues in the workplace relating to cyber security, including budget restraints. With the rate at which threats are advancing, new technologies are constantly being required to combat attacks. New technology requires a larger budget to fund both the tech itself and the talent managing it. As the levels of sophistication grow, so does the quantity of applications, and too the workload involved in monitoring them. SOAR streamlines these processes, making it more time and cost efficient.

Improve time management and productivity

The other benefit to improved time management is an increase in productivity. By using automated responses to threats, members of staff can better prioritize their time on tasks that cannot be automated.

Time can also be on the recruitment process – companies may find they are on the search for talent less often, as many aspects of the operations can be covered by SOAR software solutions and others can be conducted by the members of staff that were previously working on orchestration, for example.

Effectively manage incidents

Organizations may also find that threats and vulnerabilities are responded to faster. Incident response becomes more accurate, the time it takes is reduced and threat-risk is minimized with SOAR technology. The automated process removes human error.

Flexibility

The software can be flexible for your needs. SOAR was designed to adapt to any security system, being customizable for your environment. Multiple teams in a workforce should be able to utilize the tool with ease and access to input and read data. Data can be provided from machine to machine, email and manual input. How the data is tracked – and which data is tracked – will be dependent on what works for your operations.

Encourage collaboration

Collaboration becomes possible with SOAR security software. With response involving multiple processes to remediate threats – which SOAR aims to streamline – this will involve multiple individuals, or even teams. As we previously stated, multiple teams should have access to the SOAR stack that is used by a company.

How SOAR fits into a wider security network

SOAR software is like Security Information and Event Management (SIEM), but while they both collect data from a range of sources, SOAR's capabilities integrate with more applications – both internal and external. Due to the differences between the systems, it would be advised to combine both for a full, secure solution. Currently, SOAR platforms are often used to boost existing SIEM systems, but it is anticipated that SOAR services will become available on the platforms in the future.

Source:

- https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar
- SOAR Graphic is from https://www.gartner.com/doc/reprints?id=1-24GXYQKN&ct=201027&st=sb%20
- https://www.fireeye.com/products/helix/what-is-soar.html
- Market Guide for Security Orchestration, Automation and Response Solutions

  https://www.gartner.com/doc/reprints?id=1-24GXYQKN&ct=201027&st=sb%20

SOFTWARE ASSURANCE MATURITY MODEL (SAMM)

The OWASP mission is to provide an **effective and measurable** way for you to analyze and improve your **secure development lifecycle**. SAMM supports the complete software lifecycle and is **technology and process agnostic**.

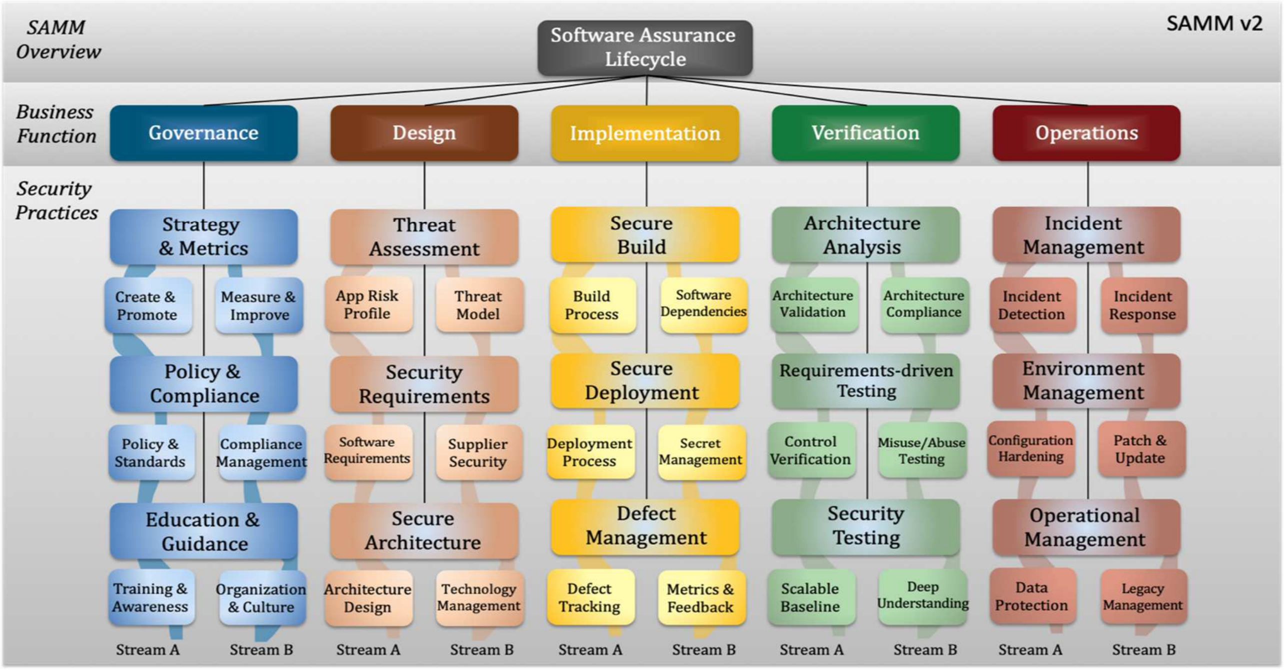
OWASP built SAMM to be **evolutive and risk-driven** in nature, as there is no single recipe that works for all organizations.

The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. The resources provided by SAMM will aid in:

- *Evaluating an organization's existing software security practices*
- *Building a balanced software security program in well-defined iterations*
- *Demonstrating concrete improvements to a security assurance program*
- *Defining and measuring security-related activities within an organization*

SAMM was defined with flexibility in mind such that it can be utilized by small, medium, and large organizations using any style of development. Additionally, this model can be applied organization-wide, for a single line-of-business, or even for an individual project.

As an open project, SAMM content shall always remain vendor-neutral and freely available for all to use. Below see the updated SAMM version 2 model:



Source:

- https://owasp.org/www-project-samm/
- https://www.opensamm.org/

SOFTWARE CONFIGURATION MANAGEMENT

Configuration management is the means to have knowledge and control over the artifacts and their state that compose a software solution. Configuration management captures and documents the current state of the software, libraries, frameworks, operating systems, patching, hardware, including versions, patch levels, configurations, documentation, and all the elements that make up a software-based solution. This is necessary for the correct and secure functionality of the solution. The basic building blocks of software configuration management are the following:

Configuration item:

A configuration item is the atom of configuration management. Configuration items are things such as software source code files, requirements documents, or program resources such as image or video files, and software libraries.

Baseline:

A baseline is an immutable set of configuration items that have immutable states. A baseline may have the properties of being associated with workflows, workload environments, conditions of approval, or qualitative states such as security.

Version:

A version is a concept that describes the immutable state of a configuration item, a set of configuration items, and a baseline. A version is associated with a change set.

Change set:

A change set is group of related changes to configuration items that have been changed, and it is the basis of how changes to the software system are controlled. Change sets are subject to code review, quality assurance, testing, verification, and acceptance measures.

Branch:

A branch in configuration management terms has two definitions. The first one is that a branch identifies a set of versioned configuration items that are being developed in parallel to the main configuration. Second, to branch is a verb where a set of configuration items are copied off for parallel development. A main branch, or trunk, is the base configuration from which all other branches are derived.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 797). Wiley. Kindle Edition.

SOFTWARE DEFINE NETWORK (SDN)

NOTE FROM CLEMENT:
This is a topic related to Micro-segmentation. It is listed in the CBK under Micro-segmentation.

SDN is an approach to network operation, design, and management that models flexibility and choice. A traditional networking concept is to configure at the device, like on a router or switch. This is complex and requires a lot of administration. Because of training and competency requirements, organizations must use one vendor or one product line to be proficient and avoid device incompatibility.

Using SDN removes the traditional networking concepts of IP addressing, subnets, routing, and the like from needing to be programmed into or deciphered by hosted applications. It also improves the ability to respond to changes in threats, to adapt quickly to dynamic physical and business conditions, and to take advantage of best available technology.

The purpose of SDN is to separate hardware and hardware-based settings from the network services of data transmission. It splits traditional network traffic into three components categorized as raw data, data transmission method, and data purpose. There are three planes, or layers, of the SDN architecture:

The idea of programmability is the basis for the most precise definition of what SDN is: technology that separates the control plane management of network devices from the underlying data plane that forwards network traffic.

IDC broadens that definition of SDN by stating: “Datacenter SDN architectures feature software-defined overlays or controllers that are abstracted from the underlying network hardware, offering intent-or policy-based management of the network as a whole. This results in a datacenter network that is better aligned with the needs of application workloads through automated (thereby faster) provisioning, programmatic network management, pervasive application-oriented visibility, and where needed, direct integration with cloud orchestration platforms.”

The driving ideas behind the development of SDN are myriad. For example, it promises to reduce the complexity of statically defined networks; make automating network functions much easier; and allow for simpler provisioning and management of networked resources, everywhere from the data center to the campus or wide area network.

Separating the control and data planes is the most common way to think of what SDN is, but it is much more than that, said Mike Capuano, chief marketing officer for Pluribus.

“At its heart SDN has a centralized or distributed intelligent entity that has an entire view of the network, that can make routing and switching decisions based on that view,” Capuano said. “Typically, network routers and switches only know about their neighboring network gear. But with a properly configured SDN environment, that central entity can control everything, from easily changing policies to simplifying configuration and automation across the enterprise."

How does SDN support edge computing, IoT and remote access?

A variety of networking trends have played into the central idea of SDN. Distributing computing power to remote sites, moving data center functions to the edge, adopting cloud computing, and supporting Internet of Things environments – each of these efforts can be made easier and more cost efficient via a properly configured SDN environment.

Typically, in an SDN environment, customers can see all of their devices and TCP flows, which means they can slice up the network from the data or management plane to support a variety of applications and configurations, Capuano said. So, users can more easily segment an IoT application from the production world if they want, for example.

Some SDN controllers have the smarts to see that the network is getting congested and, in response, pump up bandwidth or processing to make sure remote and edge components do not suffer latency.

SDN technologies also help in distributed locations that have few IT personnel on site, such as an enterprise branch office or service provider central office.

Naturally, these places require remote and centralized delivery of connectivity, visibility and security. SDN solutions that centralize and abstract control and automate workflows across many places in the network, and their devices, improve operational reliability, speed and experience.

Source:

- https://www.networkworld.com/article/3209131/what-sdn-is-and-where-its-going.html
- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 471). Wiley. Kindle Edition.

SOFTWARE-DEFINED SECURITY

This is a new term to me and a new term within the CBK. I remember running into it maybe once or twice. There is no mention of it in the official study book from ISC2.

Software-defined security is when security functions are abstracted from the hardware they run on and become **virtual network functions (VNFs)**.

This virtualization enables additional functionality such as segmentation, which adds new layers of security. While much of the security infrastructure can be virtualized, in order to further reduce vulnerabilities, security is required at a device's hardware and firmware level — for example, with silicon root of trust.

The Evolution of Software-Defined Security

First a few words about CAPEX and OPEX

Businesses have a variety of expenses, from the rent they pay for their factories or offices to the cost of raw materials for their products, to the wages they pay their workers to the overall costs of growing their business. To simplify all these costs, businesses organize them under different categories. Two of the most common are capital expenditures (CAPEX) and operating expenses (OPEX).

Capital expenditures (CAPEX) are major purchases a company makes that are designed to be used over the long-term. Operating expenses (OPEX) are the day-to-day expenses a company incurs to keep its business operational.

Software-defined security began by virtualizing security functions to run as VNFs on generic hardware. This virtualization allowed for a reduced device footprint, remote management, reduced **capex** and **opex**, and simplified deployments, and made updating the system easier.

With security function virtualization, the VNFs reside on devices as software. The devices running the VNFs can execute the same functions as the hardware they replaced, and then some.

More recently, security as code has gained traction in the IT security field. In this approach, security functions are written directly into an application or network's software instead of having separate security VNFs. Security as code is often part of DevOps approaches, often then referred to as DevSecOps. By having security as code, security approaches become part of the development process and not added on top of everything later.

Segmentation

In a virtualized network or data center, segmentation helps limit the scope of data security breaches. Operators can use network segmentation to create virtual networks for different application traffic. These virtual networks exist within a virtual network overlay.

Network segmentation prevents one application's traffic from mingling with another. A compromised application then has a harder time spreading its malicious code or viewing the other traffic.

In a secure data center, micro-segmentation separates different workloads from each other. By using micro-segmentation, east-west traffic is secured more effectively. That means communication between servers or between workloads becomes less vulnerable to attacks

Silicon Root of Trust

Also called hardware root of trust, silicon root of trust is a piece of hardware, usually a chip, that verifies all of the firmware and software that a device runs such as when a server boots up and runs BIOS. Verification is done cryptographically, and if the firmware or software stack fails the verification, it cannot access the resources on the device.

There are proprietary and open source silicon root of trust chips. Proprietary chips can be more expensive, but there is more control over the whole production line to ensure there is no tampering with chips. Open source is less expensive and organizations like Google who began the open source silicon root of trust, OpenTitan — are using vendor and platform agnostic designs.

Benefits and Drawbacks

There are many benefits to software-defined security, no matter whether an organization uses VNFs, security as code, or a combination in their network.

Software-defined security has all of the benefits seen in an SDN or an SD-WAN. With virtualization comes capabilities like centralized remote management, scalable instances, adaptable and updatable functions, and a smaller physical footprint.

Organizations that have a sprawling network have seen benefits from security virtualization at their network's edge. It makes deploying, maintaining, and updating security functions simpler and more cost-effective. Technologies such as SD-branch and secure access service edge (SASE) bring new software-defined security elements into remote locations at the network edge.

A drawback is that organizations must remember to secure the hardware and firmware levels of devices. When an organization puts all of its focus on securing environments virtually, it is easy to overlook the security needs of the remaining hardware. Silicon root of trust is one method of resolving this weak point.

Software-Defined Security: Key Takeaways

1. Software-defined security began with virtualizing security functions in order to replace the hardware with software.
2. It has begun to shift to security software as code that is written into applications and network programs.
3. A virtualized security environment allows administrators to remotely perform maintenance through centralized control.

Source:

- https://www.sdxcentral.com/security/definitions/what-is-software-defined-security/
- https://www.investopedia.com/ask/answers/112814/whats-difference-between-capital-expenditures-capex-and-operational-expenditures-opex.asp

THREAT INTELLIGENCE

This is a topic from Domain 7 – Security Operations, you will find it under 7.2 Conduct logging and monitoring activities which we have already talked about within this guide already. This includes Threat Feeds and Threat hunting.

Cyberthreat information is any information that can help an organization to identify, assess, monitor, and respond to cyber threats. Examples of cyberthreat information include indicators such as system artifacts or other "observables" associated with an attack, security alerts, threat intelligence reports, recommended security tool configurations, and other tactics, techniques, and procedures (TTPs).

Several private threat intelligence companies exist that market general or sector specific threat intelligence. In many cases, these companies are founded by individuals who formerly served in similar roles in their countries' intelligence organizations.

General threat intelligence is also freely available from many companies as well. Google's VirusTotal evaluates URLs and files for malicious content, while Project Zero identifies previously unknown flaws in vendor products. In the spirit of "responsible disclosure," Google does not release the details of the flaws to the public until after the vendor issues a patch or 90 days have passed without vendor remediation.

Threat intelligence feeds refer to continuous data streams that provide information on threats that can adversely affect an organization's security. They give security teams a list of indicators of compromise (IoCs) that includes malicious URLs, malware hashes, and malicious email and IP addresses related to attacks.

Often, the data obtained from threat intelligence feeds dictate the next steps or actions that security teams need to take to protect their organizations. These actions include blacklisting IoCs or blocking connection requests from identified threat sources and preventing malware from reaching connected systems.

Threat intelligence feeds differ from threat information, which refers to general data without contextual relevance that a security analyst or investigator can use to take the necessary action to prevent loss. They can be likened to routes on a driving app that tells the driver, which is the best way to take, depending on his/her goal (e.g., less time, no traffic, no traffic enforcers, etc.).

How Important are Threat Intelligence Feeds?

For cybersecurity experts, dealing with online threats is of utmost importance. Time is of the essence because the longer systems are exposed to a threat, the greater the damage to them may get. That makes it critical for security analysts and researchers to have access to reliable and accurate threat intelligence feeds that they can integrate with existing solutions and systems so these can more readily identify and block attack vectors.

Where do Threat Intelligence Feeds Get Data?

The best threat intelligence feeds typically obtain data from multiple sources. And so providers often engage in partnerships and agreements to share information. The more comprehensive the threat intelligence feeds are, the greater an organization's chances of preventing intrusions and compromise. We identified the most common data sources of threat intelligence feeds below.

1. Open-Source Intelligence (OSINT) Feeds

OSINT feeds have become a go-to data source for cybersecurity professionals because they are publicly available. These feeds often collate data from various communities, including those run by government departments and independent research organizations. But because they are free to access, they may need additional parsing and restructuring before they can be fed to existing systems and solutions.

Some of the most widely used OSINT feeds include Ransomware Tracker, Internet Storm Center, VirusTotal, and VirusShare Malware Reports. Threat hunters can also rely on government-sponsored feeds such as the Federal Bureau of Investigation (FBI)'s InfraGard Portal and the Department of Homeland Security's Automated Indicator Sharing.

2. Network and Application Logs

Security analysts and researchers need to compare network and application logs with IoCs to see if attempts or attacks are currently taking place against their organizations. Unauthorized access, especially those originating from known malicious sources, can be seen on these logs.

3. Third-Party Feeds

Third-party feeds are the paid counterparts of OSINT feeds. Unlike most publicly accessible feeds, however, these databases don't require further parsing or structuring. The vendors that collated them already did that for customers so they can use the feeds as is.

Examples of the third-party feeds include IBM's X-Force Exchange, Palo Alto Networks's Auto Focus, and RSA's NetWitness Suite.

Threat Hunting

Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network. Cyber threat hunting digs deep to find malicious actors in your environment that have slipped past your initial endpoint security defenses.

After sneaking in, an attacker can stealthily remain in a network for months as they quietly collect data, look for confidential material, or obtain login credentials that will allow them to move laterally across the environment.

Once an adversary is successful in evading detection and an attack has penetrated an organization's defenses, many organizations lack the advanced detection capabilities needed to stop the advanced persistent threats from remaining in the network. That is why threat hunting is an essential component of any defense strategy.

Threat hunting is becoming increasingly important as companies seek to stay ahead of the latest cyber threats and rapidly respond to any potential attacks.

Threat Hunting Methodologies

Threat hunters assume that adversaries are already in the system, and they initiate investigation to find unusual behavior that may indicate the presence of malicious activity. In proactive threat hunting, this initiation of investigation typically falls into three main categories:

1. Hypothesis-driven investigation

Hypothesis-driven investigations are often triggered by a new threat that has been identified through a large pool of crowdsourced attack data, giving insights into attackers' latest tactics, techniques, and procedures (TTP). Once a new TTP has been identified, threat hunters will then look to discover if the attacker's specific behaviors are found in their own environment.

2. Investigation based on known Indicators of Compromise or Indicators of Attack

This approach to threat hunting involves leveraging tactical threat intelligence to catalog known IOCs and IOAs associated with new threats. These then become triggers that threat hunters use to uncover potential hidden attacks or ongoing malicious activity.

3. Advanced analytics and machine learning investigations

The third approach combines powerful data analysis and machine learning to sift through a massive amount of information in order to detect irregularities that may suggest potential malicious activity. These anomalies become hunting leads that are investigated by skilled analysts to identify stealthy threats.

All three approaches are a human-powered effort that combines threat intelligence resources with advanced security technology to proactively protect an organization's systems and information.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 29). Wiley. Kindle Edition.
- https://www.techslang.com/definition/what-are-threat-intelligence-feeds/
- https://www.crowdstrike.com/cybersecurity-101/threat-hunting/
- Threat Hunting Report from Crowdstrike at https://go.crowdstrike.com/crowdstrike-2020-overwatch-threat-hunting-report.htm

TOOL SETS

This is certainly a high-level item that does not tell you much. It is within Domain 8 under 8.2 Identify and apply security controls in software development ecosystems. It is in the context of security controls within software development. I will try my best to provide info on what I believe to be included under this topic from a best practice perspective and also covering some of the best tools.

NOTE FROM CLEMENT:
The exam is product agnostic. So do not worry about tool names and vendor names. Concentrate on the best practices and what has to be done to improve security within your software development environment.

Below you have information extracted from the Center for Internet Security (CIS) top 20 CIS Controls.

This is control number 18 related to Application Software Security.

Key Takeaways for Control 18

- **Understand your risk**. The first great addition to control 18 is the requirement to run both static and dynamic code analysis utilities on in-house developed code. The second is creating the ability for vulnerabilities to be reported to the company, especially from outside parties. Both of these are going to uncover vulnerabilities to the business which previously may have remained hidden for long periods of time.
- **Layered security is important**. This is iterated repeatedly in control 18. Starting with training developers on how to write secure code, testing the code they write, harden the environment around the code, then install security tools in front of the code. The goal is to have multiple security layers to stop an attack before it can start.

Requirement Listing for Control 18:

1. Establish Secure Coding Practices

Description: Establish secure coding practices appropriate to the programming language and development environment being used.

Notes: The first step in writing secure code is following best practices. OWASP has a great cheat sheet for the secure software development life cycle. Additionally, developers can study for the ISC2 Certified Secure Software Lifecycle Professional (CSSLP) certification.

2. Ensure Explicit Error Checking is Performed for All In-house Developed Software

Description: For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

Notes: Many common attacks against software come in the form of no sanitizing user input or not handling errors correctly. Both can have devastating effects on the security of the software and underlying operating system. Following section 7 lower down can help catch many of these if they are inadvertently left in the source code.

3. Verify That Acquired Software is Still Supported

Description: Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.

Notes: This is the same as Control 2.2. Complex software used in enterprises is bound to have a vulnerability discovered sooner or later. Having software which is receiving security updates will ensure that your network is not unnecessarily left exposed. In some instances, the business will require the use of unsupported software, such as Windows XP. If that is the case, make sure you leverage compensating controls to limit the risk exposure to the business.

4. Only Use Up to date And Trusted Third-Party Components

Description: Only use up-to-date and trusted third-party components for the software developed by the organization.

Notes: It is one thing to make sure the software is still supported; it is entirely different to make sure that you actually install updates to that software. You should install updates to supported software as soon as possible.

5. Use Only Standardized and Extensively Reviewed Encryption Algorithms

Description: Use only standardized and extensively reviewed encryption algorithms.

Notes: There are plenty of encryption algorithms which have been studied by mathematicians many times over. Creating a proprietary encryption algorithm is introducing unnecessary risk that sensitive data can be arbitrarily decrypted by any number of flaws in the algorithm or usage of the encryption.

6. Ensure Software Development Personnel are Trained in Secure Coding

Description: Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.

Notes: It is easier and cheaper to write secure code from the beginning rather than being notified of a vulnerability by QA or a customer. Training is essential in reducing the cost of finding and remediating vulnerabilities in source code.

7. Apply Static and Dynamic Code Analysis Tools

Description: Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.

Notes: Because humans are fallible creatures, it is important to test for mistakes that have been made. Both dynamic and static code analysis tools have their pros and cons. Research both to determine which may be right for your code.

8. Establish a Process to Accept and Address Reports of Software Vulnerabilities

Description: Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.

Notes: You should not rely on your QA team finding all of your security vulnerabilities. Even if your organization does not write any application software, websites can be littered with security bugs that can open the door for attackers all over the world. Create, document, and publish how anyone can submit a security issue to your company.

9. Separate Production and Non-Production Systems

Description: Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.

Notes: Ideally, the developers should write the code, QA should test the code, and operations should move the code into the production environment. In smaller organizations, anyone who has the ability to push code into production should have all of their actions monitored when doing so.

10. Deploy Web Application Firewalls (WAFs)

Description: Protect web application by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.

Notes: Deploying a web application firewall was consolidated from a handful of sections into a single section with version 7 of the CIS Controls. The higher-level view eliminates the controls for specific vulnerabilities, opting instead for a broad stroke of protecting against attacks with a tool. WAFs can be incredible powerful to protect against the missed input sanitization bug a developer left in on a Friday afternoon.

11. Use Standard Hardening Configuration Templates for Databases

Description: For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

Notes: As with Control 5, deploying hardening guides from either CIS or DISA against everything possible will help reduce the attack surface down as much as possible.

See how simple and effective security controls can create a framework that helps you protect your organization and data from known cyber-attack vectors by downloading this guide here.

APPLICATION SECURITY CONTROLS

Identifying and managing Application Security Controls (ASCs) or security requirements and security issues are essential aspects of an effective secure software development program. Clear and actionable technical controls that are continuously refined to reflect development processes and changes in the threat environment are the foundation upon which SDL tools and process are built.

The practices listed in this document and application security controls they drive will lead to the identification of software design or implementation weaknesses, which when exploited expose the application, environment or company to a level of risk. These issues must be tracked (see Manage Security Findings) and action must be taken to improve the overall security posture of the product. Further, effective tracking supports the ability to both gauge compliance with internal policies and external regulations and define other security assurance metrics.

Actively Manage Application Security Controls

Regardless of the development methodology being used, defining application security controls begins in (or even before) the Design stage and continues throughout an application’s lifecycle in response to changing business requirements and an ever-evolving threat environment.

The inputs used to identify the necessary security requirements should include the secure design principles described in the following section and feedback from the established vulnerability management program, and may also require input from other stakeholders, such as a compliance team (e.g., if the application must comply with standards such as HIPAA, PCI, GDPR, etc.) or an operations and deployment team, because where and how the application is deployed may affect its security needs.

At a high level, the workflow should include:

- Identifying threats, risks and compliance drivers faced by this application
- Identifying appropriate security requirements to address those threats and risks
- Communicating the security requirements to the appropriate implementation teams
- Validating that each security requirement has been implemented
- Auditing, if required, to demonstrate compliance with any applicable policies or regulations

Secure Design Principles

The principles of secure system design were first articulated in a 1974 paper by Jerome Saltzer and Michael Schroeder (The Protection of Information in Computer Systems) The principles from that paper that have proven most important to the designers of modern systems are:

- Economy of mechanism: keep the design of the system as simple and small as possible.
- Fail-safe defaults: base access decisions on permission (a user is explicitly allowed access to a resource) rather than exclusion (a user is explicitly denied access to a resource).
- Complete mediation: every access to every object must be checked for authorization.
- Least privilege: every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- Least common mechanism: minimize the amount of mechanism common to more than one user and depended on by all users.
- Psychological acceptability: it is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.
- Compromise recording: it is sometimes suggested that mechanisms that reliably record that a compromise of information has occurred can be used in place of more elaborate mechanisms that completely prevent loss.

In the years since Saltzer and Schroeder published their paper, experience has demonstrated that some additional principles are important to the security of software systems. Of these, the most important are:

- Defense in depth: design the system so that it can resist attack even if a single security vulnerability is discovered or a single security feature is bypassed. Defense in depth may involve including multiple levels of security mechanisms or designing a system so that it crashes rather than allowing an attacker to gain complete control.
- Fail securely: a counterpoint to defense in depth is that a system should be designed to remain secure even if it encounters an error or crashes.
- Design for updating: no system is likely to remain free from security vulnerabilities forever, so developers should plan for the safe and reliable installation of security updates.

The principles described above are relevant to the design of any system, whether for client or server, cloud service, or Internet-of-Thing's device. The specifics of their application will vary – a cloud service may require multiple administrative roles, each with its own least privilege, while an IoT device will require special considerations of the need for security updates and of the need to fail securely and safely. But the principles are general and provide valuable security guidance for the designers and architects of all classes of systems.

Source:

- https://www.tripwire.com/state-of-security/security-data-protection/security-controls/20-critical-security-controls-control-18-application-software-security/
- Top 20 CIS Controls and resources at https://www.cisecurity.org/controls/cis-controls-list/
- https://safecode.org%2Fwp-content%2Fuploads%2F2018%2F03%2FSAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf&usg=AOvVaw2ygsTZpQiKbyu5sE8j1wOB

TRUST BUT VERIFY

NOTE FROM CLEMENT:
This is a concept used in computer security for a long period of time. Today it is being challenge and new threats such as persistent threats and others have change this to “Never trust, Always verify” such as you have seen in the section on Zero Trust Architecture a bit earlier in this document.

In 1987 at the INF (Intermediate-Range Nuclear Forces Treaty), President Ronald Reagan used an old Russian phrase that Premier Vladimir Lenin originated, ‘doveryai, no proveryai,’ which translate to ‘trust, but verify.’ This phrase frequently used by President Reagan when he discussed the relations between the United States and the Soviet Union, it became one of his greatest quotes. Almost four decades later, it still applies in many circumstances. One of these circumstances is leveraging threat intelligence to protect the network. It can be applied to your own personal life as well as Cybersecurity.

Threat intelligence helps to determine whether a threat is viable or not, and other pertinent information that is critical in protecting networks and data. A simple example is verifying an individual entering a country with a passport. Is the passport valid? Is this person a threat to national security? What information was used to determine if this person is a potential threat or not? The answer is verification through intelligence.

Verification can be used in various forms, for example, physical security can entail biometrics, visual identification, and IDs, to determine the trustworthiness of an individual. In network security, trust must be enabled for one to access the network to send and receive data within systems. So, what is the best way to help prevent network infiltration and data exfiltration? Implementing Zero-trust inspection of all traffic that leverages proactive intelligence is the most advanced strategy for network security.

Shielding and Advanced Threat Detection using dynamic intelligence on a mass-scale dramatically increase an organization’s cyber security posture. Gaining visibility into threats enables cyber security teams to create policies that harden network defenses. Today’s environment has become extremely challenging since much of the workforce remote that has created new and more persistent threats. Also, overcoming the skills gap, tightened budgets, and maintaining compliance are ongoing. So, in the immortal words of Ronald Reagan, the best way to keep the network safe is to ‘trust but verify.’

Source:

- https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify
- https://www.centripetal.ai/blog/trust-but-verify

USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)

What is UEBA?

Hackers can break into firewalls, send you e-mails with malicious and infected attachments, or even bribe an employee to gain access into your firewalls. Old tools and systems are quickly becoming obsolete, and there are several ways to get past them.

User and entity behavior analytics (UEBA) give you more of a comprehensive way to make sure that your organization has top-notch IT security, while also helping you detect users and entities that might compromise your entire system.

A Definition of User and Entity Behavior Analytics

User and entity behavior analytics, or UEBA, is a type of cyber security process that takes note of the normal conduct of users. In turn, they detect any anomalous behavior or instances when there are deviations from these “normal” patterns. For example, if a particular user regularly downloads 10 MB of files every day but suddenly downloads gigabytes of files, the system would be able to detect this anomaly and alert them immediately.

UEBA uses machine learning, algorithms, and statistical analyses to know when there is a deviation from established patterns, showing which of these anomalies could result in a potential, real threat. UEBA can also aggregate the data you have in your reports and logs, as well as analyze file, flow, and packet information.

In UEBA, you do not track security events or monitor devices; instead, you track all the users and entities in your system. As such, UEBA focuses on insider threats, such as employees who have gone rogue, employees who have already been compromised, and people who already have access to your system and then carry out targeted attacks and fraud attempts, as well as servers, applications, and devices that are working within your system.

Benefits of UEBA

It is the unfortunate truth that today's cyber security tools are fast becoming obsolete, and more skilled hackers and cyber attackers are now able to bypass the perimeter defenses that are used by most companies. In the old days, you were secure if you had web gateways, firewalls, and intrusion prevention tools in place. This is no longer the case in today’s complex threat landscape, and it is especially true for bigger corporations that are proven to have very porous IT perimeters that are also very difficult to manage and oversee.

The bottom line? Preventive measures are no longer enough. Your firewalls are not going to be 100% foolproof, and hackers and attackers will get into your system at one point or another. This is why detection is equally important: when hackers do successfully get into your system, then you should be able to detect their presence quickly in order to minimize the damage.

How UEBA Works

The premise of UEBA is quite simple. You can easily steal an employee’s username and password, but it is much harder to mimic the person’s normal behavior once inside the network.
For example, let us say you steal Jane Doe’s password and username. You would still not be able to act precisely like Jane Doe once in the system, unless given extensive research and preparation. Therefore, when Jane Doe’s username is logged in to the system, and her behavior is different than that of typical Jane Doe, that is when UEBA alerts start to sound.

Another relatable analogy would be if your credit card was stolen. A thief can pickpocket your wallet and go to a high-end shop and start spending thousands of dollars using your credit card. If your spending pattern on that card is different from the thief’s, the company’s fraud detection department will often recognize the abnormal spending and block suspicious purchases, issuing an alert to you or asking you to verify the authenticity of a transaction.

As such, UEBA is a particularly important component of IT security, allowing you to:

Detect insider threats.
It is not too far-fetched to imagine that an employee, or perhaps a group of employees, could go rogue, stealing data and information by using their own access. UEBA can help you detect data breaches, sabotage, privilege abuse, and policy violations made by your own staff.

Detect compromised accounts.
Sometimes, user accounts are compromised. It could be that the user unwittingly installed malware on his or her machine, or sometimes a legitimate account is spoofed. UEBA can help you weed out spoofed and compromised users before they can do real harm.

Detect brute-force attacks.
Hackers sometimes target your cloud-based entities as well as third-party authentication systems. With UEBA, you are able to detect brute-force attempts, allowing you to block access to these entities.

Detect changes in permissions and creation of super users.

Some attacks involve the use of super users. UEBA allows you to detect when super users are created, or if there are accounts that were granted unnecessary permissions.

Detect breach of protected data.
If you have protected data, it is not enough to just keep it secure. You should know when a user accesses this data when he or she does not have any legitimate business reason to access it.

UEBA vs. SIEM

Security Information and Event Management, or SIEM, is the use of a complex set of tools and technologies that gives a comprehensive view of the security of your IT system. It makes use of data and event information, allowing you to see patterns and trends that are normal, and alert you when there are anomalous trends and events. **UEBA works the same way, only that it uses user (and entity) behavior information to come up with what's normal and what's not.**

SIEM, however, is rules-based, and advanced hackers can easily work around or evade these rules. What is more, SIEM rules are designed to immediately detect threats happening in real time, while advanced attacks are usually carried out over a span of months or years. UEBA, on the other hand, does not rely on rules. Instead, it uses risk scoring techniques and advanced algorithms, allowing it to detect anomalies over time.

One of the best practices for IT security is to use both SIEM and UEBA to have better security and detection capabilities.

Best Practices for UEBA

UEBA arose out of the malicious behavior by users and other entities. UEBA tools and processes are not meant to replace earlier monitoring systems, but instead should be used to complement them and enhance your company’s overall security posture.

Another great practice is to harness the storage and computational powers of big data, using machine learning and statistical analysis to prevent getting an avalanche of useless alerts and become overwhelmed with the large volume of data generated.

UEBA uses machine learning and algorithms to strengthen security by monitoring users and other entities, detecting anomalies in behavior patterns that could be indicative of a threat. By taking a more proactive approach to security and gaining more visibility into user and entity behavior, today’s enterprises can build a stronger security posture and more effectively mitigate threats and prevent security breaches.

Source:

- https://www.code42.com/resources/infographic-six-unusual-data-behaviors-that-indicate-insider-threat/?utm_content=unusual%20data%20behaviors%20infographic&utm_source=g

oogle&utm_medium=cpc&utm_campaign=ENT_Alternate%20Solutions%20-%20Search&utm_term=user%20entity%20behavior%20analytics&_bt=513224854687&_bk=%2Buser%20%2Bentity%20%2Bbehavior%20%2Banalytics&_bm=b&_bn=g&_bg=114485250899&gclid=CjwKCAjwmv-DBhAMEiwA7xYrd5s68bFBUG8kB359gJxLvdOVehx3Q03CW8BZznxp_7ZX6UxYQsCj4RoC9RkQAvD_BwE

- https://digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more

VIRTUAL EXTENSIBLE LOCAL AREA NETWORK (VXLAN)

NOTE FROM CLEMENT:
This is a topic related to Micro-segmentation. It is listed in the CBK under Micro-segmentation.

What is VXLAN?

VXLAN is an encapsulation protocol that provides data center connectivity using tunneling to stretch Layer 2 connections over an underlying Layer 3 network.

In data centers, VXLAN is the most used protocol to create overlay networks that sit on top of the physical network, enabling the use of virtual networks. The VXLAN protocol supports the virtualization of the data center network while addressing the needs of multi-tenant data centers by providing the necessary segmentation on a large scale.

What Problem Does VXLAN Solve?

Data centers have rapidly increased their server virtualization over the past decade, resulting in dramatic increases in agility and flexibility. Virtualization of the network and decoupling the virtual network from the physical network makes it easier to manage, automate, and orchestrate.

VXLAN is a technology that allows you to segment your networks (as VLANs do) but also solves the scaling limitation of VLANs and provides benefits that VLANs cannot. Some of the important benefits of using VXLANs include:

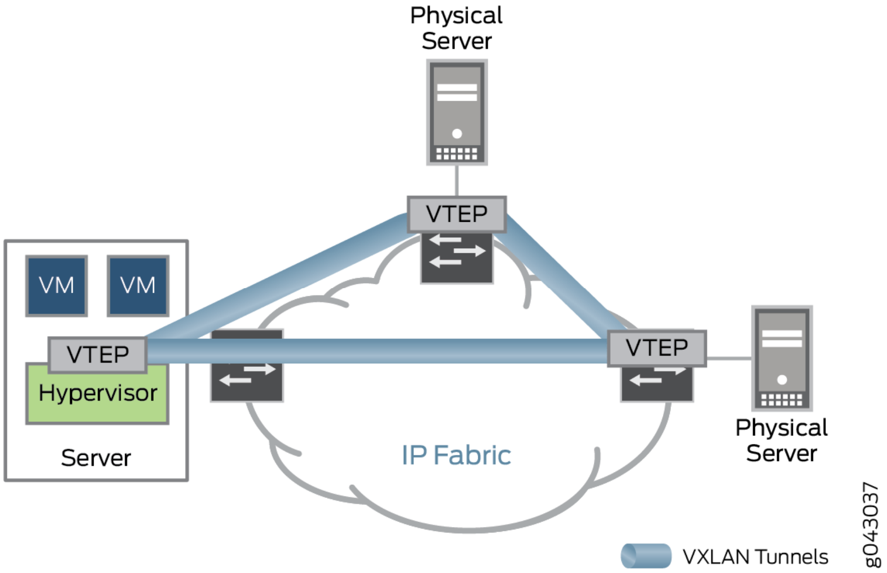
- You can theoretically create as many as 16 million VXLANs in an administrative domain (as opposed to 4094 VLANs).
- VXLANs provide network segmentation at the scale required by cloud builders to support exceptionally large numbers of tenants.
- With traditional Layer 2 networks you are constrained by Layer 2 boundaries and forced to create large or geographically stretched Layer 2 domains. VXLAN's functionality allows you to dynamically allocate resources within or between data centers and enables migration of virtual machines between servers that exist in separate Layer 2 domains by tunneling the traffic over Layer 3 networks.

How Does VXLAN Work?

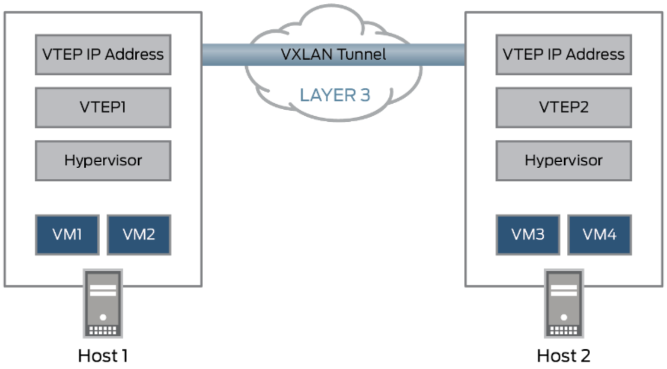
The VXLAN tunneling protocol that encapsulates Layer 2 Ethernet frames in Layer 3 UDP packets, enables you to create virtualized Layer 2 subnets, or segments, that span physical Layer 3 networks. Each Layer 2 subnet is uniquely identified by a **VXLAN network identifier (VNI)** that segments traffic.

The entity that performs the encapsulation and decapsulation of packets is called a **VXLAN tunnel endpoint (VTEP)**. To support devices that cannot act as a VTEP on their own, like bare-metal servers, a Juniper Networks device can encapsulate and de-encapsulate data packets. This type of VTEP is known as a hardware VTEP. VTEPs can also reside in hypervisor hosts, such as kernel-based virtual machine (KVM) hosts, to directly support virtualized workloads. This type of VTEP is known as a software VTEP.

Hardware and software VTEPs graphic:



In the figure below, when VTEP1 receives an Ethernet frame from Virtual Machine 1 (VM1) addressed to Virtual Machine 3 (VM3), it uses the VNI and the destination MAC to look up in its forwarding table for the VTEP to send the packet to. VTEP1 adds a VXLAN header that contains the VNI to the Ethernet frame, encapsulates the frame in a Layer 3 UDP packet, and routes the packet to VTEP2 over the Layer 3 network. VTEP2 decapsulates the original Ethernet frame and forwards it to VM3. VM1 and VM3 are completely unaware of the VXLAN tunnel and the Layer 3 network between them.



Source:

- https://www.juniper.net/us/en/products-services/what-is/vxlan/
- RFC 7348 Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks at https://tools.ietf.org/html/rfc7348

VIRTUALIZED SYSTEMS

NOTE FROM CLEMENT:
Under this topic you would also include Virtual Networks. Virtualization allow for system and data resiliency; virtualization presents security benefits.

Backups of the entire system are easier to make and recover than the physical systems.

Errors or problems in virtual systems are easily remedied. Developers and system owners can typically tear down and rebuild virtual environments in minutes because of the architecture and technologies. If a virtual system is compromised, the operating system is rarely impacted, and remediation is quick and efficient.

Virtualization has made a dramatic impact in a very short time on IT and networking and has already delivered huge cost savings and return on investment to enterprise data centers and cloud service providers. Typically, the drivers for machine virtualization, including multi-tenancy, are better server utilization, data center consolidation, and relative ease and speed of provisioning. Cloud service providers can achieve higher density, which translates into better margins. Enterprises can use virtualization to shrink capital expenditures on server hardware as well as to increase operational efficiency.

Some think that virtualized environments are more secure than traditional ones for the following reasons:

- Isolation between virtual machines (VMs) provided by the hypervisor
- No known successful attacks on hypervisors save for theoretical ones, which require access to the hypervisor source code and ability to implement it
- Ability to deliver core infrastructure and security technologies as virtual appliances such as network switches and firewalls
- Ability to quarantine and recover quickly from incidents

Others think that the new virtualized environment requires the same type of security as traditional physical environments. As a result, it is not uncommon to see legacy security solutions, processes, and strategies applied to the virtual environment. The bottom line, though, is that the new environment is more complex and requires a new approach to security.

As enterprises embark on their virtualization journeys, it is critical to review existing processes and develop strategies to address security risks across physical and virtual environments in order to ensure compliance and security visibility in the data center.

Cloud Computing Top Threats

In the Cloud Computing Top Threats report by CSA2, experts identified the following nine critical threats to cloud security (ranked in order of severity):

1. Data breaches
2. Data loss
3. Account or service traffic hijacking
4. Insecure interfaces and APIs

5. Denial of services
6. Malicious insiders
7. Abuse of cloud services
8. Insufficient due diligence
9. Shared technology vulnerabilities

Virtualization Risks and Controls

This section details the various virtualization risks and recommended security controls for securing a virtualization environment. Key virtualization vendors and other stakeholders assisted in the identification of these security risks and countermeasures.

While virtualization provides numerous benefits using VMs, moving to a virtualized environment does not exempt IT systems from the security risks applicable to such setup in a physical environment. Furthermore, the use of VMs may introduce new and unique security risks or lead to more significant impacts for known risks. Consequently, as part of assessing the risks of virtualization, the following should be considered:

Risk 1 – VM Sprawl

Uncontrolled proliferation of VMs can lead to an unmanageable condition of unpatched and unaccounted-for machines.

Risk 2 – Sensitive Data Within a VM

Data confidentiality within VMs can be easily compromised because data can be easily transported and tampered with.

Risk 3 – Security of Offline and Dormant VMs

Dormant and offline VMs can eventually deviate so far from a current security baseline that simply powering them on introduces massive security vulnerabilities.

Risk 4 – Security of Pre-Configured (Golden Image) VM / Active VMs

VMs exist as files on a virtualization platform, which can lead to unauthorized access, resulting in machine configuration changes or viral payload injection into the platform’s virtual disks.

Risk 5 – Lack of Visibility Into and Control Over Virtual Networks

Software-defined virtual networks can cause network security breaches, because traffic over virtual networks may not be visible to security protection devices on the physical network.

Risk 6 – Resource Exhaustion

Uncontrolled physical resource consumption by virtual processes can lead to reduced availability.

NOTE:

A risk factor unique to virtual environments is the hypervisor. Hypervisor is the software and/or firmware responsible for hosting and managing VMs. It provides a single point of access into the virtual environment and is also potentially a single point of failure. A misconfigured hypervisor can result in a single point of compromise of the security of all its hosted components. It does not matter how individual VMs are hardened—a compromised hypervisor can override those controls and provide a convenient single point of unauthorized access to all the VMs. The following security risks related to the use of hypervisor should be considered by those planning to use or currently using virtual technologies:

Risk 7 – Hypervisor Security

Hypervisor security is the process of ensuring that the hypervisor, the software that enables virtualization, is secure throughout its life cycle, including development, implementation, provisioning, and management.

Risk 8 – Unauthorized Access to Hypervisor

Administrative access controls to the hypervisor may not be adequate to protect against potential hacker attacks. Compared to traditional IT environments, virtualization of IT systems inevitably leads to changes in operational procedures. As a result, some common defense-in-depth practices used in securing physical servers may be affected or ignored, while newly introduced features or functions may expose the environment to additional risks. The following security risks related to changes in operation procedures should be considered:

Risk 9 – Account or Service Hijacking Through the Self-Service Portal

Portal vulnerabilities can lead to privilege escalation attacks.

Risk 10 – Workloads of Different Trust Levels Located on the Same Server

Ensure that there is sufficient security segregation of workloads on a physical host. Some enterprise information and communication personnel may elect to apply virtualization technologies through outsourcing services from cloud service providers. In such cases, it may be necessary to consider additional risk factors, including the following.

Risk 11 – Risk Due to Cloud Service Provider APIs

A hybrid (private / public) cloud virtualization implementation can pose security risks due to account / authentication federation.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 470). Wiley. Kindle Edition.
- https://www.networkcomputing.com/data-centers/top-11-virtualization-risks-identified
- https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for%20_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf

VOICE OVER INTERNET PROTOCOL (VOIP)

Voice over Internet Protocol (VoIP) is a method using several technologies to encapsulate voice communications and multimedia sessions over IP networks.

VoIP has become a popular and inexpensive way for companies and individuals to operate telephony solution using a TCP/IP network connection.

VoIP technology is not automatically any more secure than analog. It is essentially plain-form communications and is easily intercepted and eavesdropped. With adequate configuration, highly encrypted solutions are possible, and attempts to interfere or wiretap are deterred. Even then, VoIP still requires the attention of security professionals.

VoIP has been the target of numerous attacks and there are a lot of readily available tools on the Internet that can be downloaded for free. See the following page to read more details about common attacks related to VoIP using Linux and freeware tools: https://hakin9.org/voip-hacking-techniques/

VoIP Fundamental Protocols

VoIP telephony uses mainly two protocols in order to set up a call and to transport Audio/Video signal. They are described in the following subsections.

Real-Time Protocol (RTP)

The Real-time Transport Protocol (RTP) is a standardized packet format used by IP networks in order to deliver audio/video signal. RTP was developed by the Audio/Video Transport working group of Internet Engineering Task Force (IETF) standards organization, it was initially described in IETF RFC 1889 and then superseded by IETF RFC 3550. It was designed for end-to-end, real-time; transfer of stream data and it’s regarded as the primary standard for audio/video transport in IP networks and it is used with an associated profile and payload format.

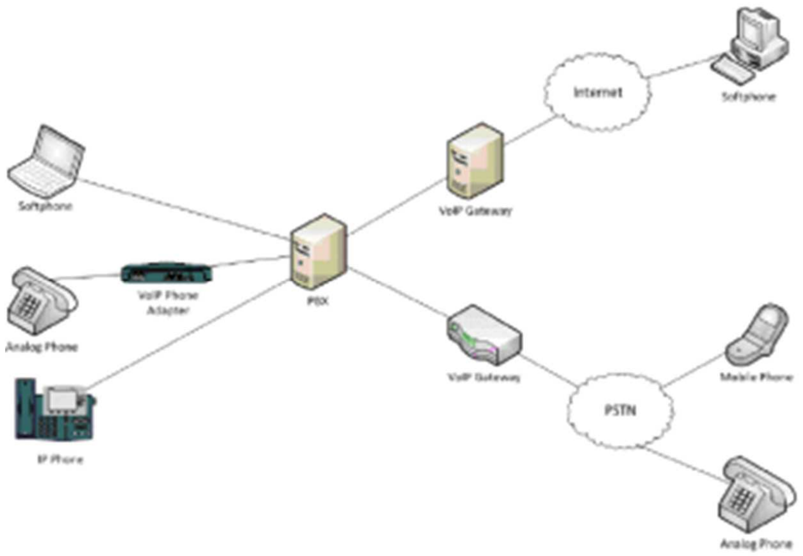


Figure 1. Classic VoIP network scenario

RTP is used in conjunction with the Real-Time Control Protocol (RTCP) which is used to monitor transmission statistics and Quality of Service aiding synchronization of multiple streams. While RTP is originated and received on even port numbers, the associated RTCP packets use the next higher odd port number.

The protocol provides facilities for jitter compensation (jittering is rather common on a Packet-Switched Network since communication is provided by network Routers), detection of out of sequence arrival in data and allows data transfer to multiple destinations through IP multicast.

Real-time applications require timely delivery of information and can tolerate some packet loss usually than an excessive delay. Thus, in order to achieve this goal, the Transmission Control Protocol (TCP) is normally not used by RTP since TCP favors reliability over timeliness, RTP systems are instead usually built on the User Datagram Protocol (UDP).

The audio sampling rate is typically either 8000Hz or 16000Hz and the rate that RTP packets are transmitted is determined by the audio Codec by mean of its Packetization Period. Whether those packets arrive at a fixed rate at the receiving endpoint depends on the network performance. RTP packets might be lost by Routers, might arrive at the receiving endpoint out of sequence, or could be even duplicated when they transit through the network.

Hence receiving endpoints are designed with the assumption that RTP packets will not arrive at the precise rate they were transmitted. About this reason an endpoint incorporate a Jitter Buffer having parameters in order to manipulate the characteristics of time buffering in an attempt to produce the highest Quality of Service during the playback. Jitter Buffer uses RTP header information to accomplish its functions.

Session Initiation Protocol (SIP)

SIP is being developed by the SIP Working Group, within the IETF, the protocol is published as IETF RFC 2543. SIP is a telephone signaling protocol used by VoIP in order to initiating, managing, and terminating voice sessions in Packet Switched Networks. SIP sessions involve one or more participants and can use either unicast or multicast communication. SIP is text-encoded and highly extensible since it may be extended to accommodate features and services such as call control services, mobility and interoperability with existing telephony systems.

That are 4 types of logical SIP entities, each one participates in SIP communication as a client (the entity which initiates the Requests), as a server (the entity which Responds to Requests), or as both. One network device can have the functionality of more than one logical SIP entity. In the following the 4 types of logical SIP entities are reported:

- **USER AGENT (UA):** initiate and terminate sessions by exchanging Requests and Responses. UA is an application, which contains both a User Agent Client (UAC) and User Agent Server (UAS). UAC is a client application that initiates SIP requests while UAS is a server application that contacts the user when a SIP request is received and that returns a response on behalf of the user. Devices with UA functions are: workstations, IP-phones, Media Gateways, call agents and automated answering services;
- **PROXY SERVER:** intermediary entity that acts as both a server and a client with the purpose of making Requests on behalf of other clients. Requests are serviced either internally or by passing them on (possibly after translation) to other servers. A Proxy interprets and, when it's necessary, rewrites a Request message before forwarding it;
- **REDIRECT SERVER:** server that accepts a SIP Request, maps the SIP address of the called party into zero (if there isn't known address) or more new addresses and returns them to the client. It does not not pass the Request on to other servers;
- **REGISTRAR:** accepts REGISTER Requests in order to updating a location database with the contact information of the user specified in the Request.

There are two types of SIP messages:

- Request Messages: they are sent from the client to the server;
- Response Messages: they are sent from the server to the client.

Source:

- Warsinske, John. The Official (ISC)2 Guide to the CISSP CBK Reference (p. 451). Wiley. Kindle Edition.
- https://hakin9.org/voip-hacking-techniques/

ZERO TRUST ARCHITECTURE

Zero Trust is a strategic cybersecurity model designed to protect modern digital business environments, which increasingly include public and private clouds, SaaS applications, DevOps, robotic process automation (RPA) and more. Zero Trust is centered on the belief that organizations should not automatically trust anything, whether it is outside or inside its network perimeter. Zero Trust models demand that anyone and everything trying to connect to an organization's systems must first be verified before access is granted. The main objective of Zero Trust is to mitigate the risk of cyber-attacks in the modernized environments in which most organizations operate.

Industry analyst John Kindervag coined the phrases "Zero Trust" and "Zero Trust architectures" in 2010. This "never trust, always verify" concept quickly began to take hold and soon large enterprises, such as Google, began architecting their own interpretation of the Zero Trust model. After the massive U.S. Office of Personnel Management (OPM) breach, the House of Representatives recommended that government agencies adopt Zero Trust frameworks to protect against cyber-attacks.

The Zero Trust model largely discounts the traditional "castle and moat" approach to cybersecurity, which focused on defending the perimeter, keeping attackers out, while assuming that everyone and everything inside the perimeter was cleared for access and, therefore, did not pose a threat to the organization. This approach relied heavily on firewalls and similar security measures but was defenseless against the threat of bad actors inside organizations who gained — or were given — access to privileged accounts.

Today's technology ecosystem has been made more complex by digital transformation and, consequently, necessitates adjustments to traditional security strategies. As the attack surface grows, perimeter-focused methods are increasingly ineffective. Furthermore, remote vendors often require privileged access to critical internal systems and keeping track of who needs access to what can be increasingly difficult. In contrast, Zero Trust is enforced from everywhere to ensure the only right users and non-human identities can access the data and only the data they need, when they need it. In **Zero Trust frameworks, a "software-defined perimeter"** provides secure privileged access to human and non-human identities – regardless of where they are, which endpoint devices or machines are being used or where the data and workloads are hosted (on premise, in the cloud or in hybrid environments).

How to Implement Zero Trust in Your Organization

There is no one Zero Trust technology. Effective Zero Trust strategies utilize a mix of existing technologies and approaches, such as multifactor authentication (MFA), identity and access management (IAM), Privilged Access Management (PAM) and network segmentation, for comprehensive defense-in-depth. Zero Trust also emphasizes governance policies such as the principle of least privilege.

To build out modern architectures that align with Zero Trust, organizations often take a phased, programmatic approach over time, which involves some or all the following steps:

Protect high-power privileged accounts. It is well established that the majority of insider threat and external attacks involve privileged access abuse. Organizations should identify the most important privileged accounts, credentials and secrets across their environment and pinpoint potential weaknesses and vulnerabilities that could jeopardize their most sensitive data and critical infrastructure. With this intelligence, they can implement access controls for protecting the privileged accounts that present the most risk as it relates to Zero Trust. Over time, they can extend protections to other users and applications across the enterprise, in the cloud, at the endpoint and throughout the DevOps pipeline.

Implement multi-step authentication for business-critical assets. In Zero Trust models, Tier 0 assets must be protected above all else. Continuous multi-factor authentication (MFA) is essential in narrowing the focus of trust for users and devices. Additionally, step-up or just-in-time authentication and managerial approval processes that enable the authentication of privileged users at the exact point of access help to mitigate the risk of privileged credential-based attacks.

Strengthen endpoint security. If a malicious attacker or insider gains access to a privileged credential, he or she will appear to be a trusted user. This makes it difficult to detect high-risk activity. In combination with endpoint detection and response, anti-virus/Next Generation Anti-virus (NGAV), application patching and OS patching, organizations can reduce the risk of attacks by managing and securing privileges on endpoint devices. Additionally, organizations should implement restriction models that only trust specified applications run by specific accounts under specific circumstances. This will help mitigate the risk of ransomware and code injection attacks.

Monitor the privileged pathway. Continuous monitoring of the privileged access pathway prevents malicious insiders and external attackers from progressing their attack. Organizations should place tight controls around what end users can access; create isolation layers between endpoints, applications, users and systems – and continuously monitor access to reduce the attack surface.

Implement the principle of least privilege. It's essential to know who (among both human and non-human users) has access to what assets when and which actions they can perform. Organizations should enforce the principle of least privilege broadly along with attribute-based access controls that combine enterprise-level policy with specific user criteria to balance security with usability.

Forrester Five Steps Model

- Forrester has outlined a roadmap for a successful zero trust implementation. Here is Forrester's five step model, paraphrased:
- Identify your sensitive data at rest and in motion

    - Perform data discovery and classification
    - Segment and zone the network based on data classification
  - Map the acceptable routes for sensitive data access and egress
    - Classify all resources involved in the electronic exchange of sensitive data
    - Evaluate the workflow of data and redesign, if necessary
    - Verify the existing workflows, like PCI architectures, and verify designs
  - Architect zero trust micro-perimeters
    - Define micro-perimeters, zones, and segmentation around sensitive data
    - Enforce segmentation using physical and virtual security controls
    - Establish access based on these controls and the micro-perimeter designs
    - Automate rule and access policy baselines
    - Audit and log all access and change control
  - Monitor the zero trust environment, in detail, with security analytics
    - Leverage and identify existing security analytics solutions already existing within the organization
    - Determine the logical architecture and best placement for your security analytics tools
    - If a new solution is needed, identify a vendor that is moving in the same security direction as your organization and that can provide analytics for your other security solutions
  - Embrace security automation and adaptive response
    - Translate business process into technology automation
    - Document, assess, and test security operation center policies and procedures for effectiveness and response
    - Correlate policies and procedures with security analytics automation and determine what can be lifted from manual processes.
    - Verify the security and implementation of automation within your environment and current solutions

Source:

- CyberArk Glossary at: https://www.cyberark.com/what-is/zero-trust/
- Forrester five steps model to zero trust implementation

- After your exam if you wish to Learn More About Zero Trust, look at:

- Zero Trust Part I: The Evolution of Perimeter Security
- Zero Trust Part II: The Evolution of Trust and Five Key Considerations
- Breaking the Cycle of Security Failure with Zero Trust

ZIGBEE

Syncing up all the top smart home devices is not easy, and it requires a common language to bind together a wealth of tech from different manufacturers.

That is where Zigbee comes in – it is one of the leading protocols in helping smart home hubs control the tech in your home. If the name is familiar, it's because it has been in the news, as the Zigbee Alliance is teaming up with the likes of Google, Apple and Amazon on a new smart home standard.

If it is even more familiar it is because Amazon is starting to add a Zigbee hub into the mix on more and more of its devices, such as the new Amazon Echo.

What is Zigbee?

Right, let's start by trying to cover smart home protocols without dying of boredom. They are how your smart sensors, bulbs, hubs and cameras all talk to each other – and to you – quickly and securely.

They are necessary because the protocols you are more familiar with, such as Wi-Fi and Bluetooth, are not great for meshing together a lot of low power devices spread all around your home.

A better solution was required, and Zigbee along with Z-Wave is the answer.

What is so good about Zigbee?

Zigbee uses the IEEE's 802.15.4 personal-area network (PAN) standard to communicate with other Zigbee devices. These can talk up to a maximum range of 300+ meters with a clear line of sight, which works out to between 75-100 meters indoors with obstacles such as walls.

Zigbee creates a mesh, where each interoperable device becomes a sort of outpost, able to communicate with the next device.

Because we are going to end up having a lot of devices and sensors in our home, Zigbee needs to be able to support a lot of devices on the network, and luckily, it will cope with 65,000 at any given time. That should just about cover it 😊.

Without the need for a centralized hub, it's theoretically possible for devices to work over a huge area, passing on information around the mesh. However, not all Zigbee devices act as repeaters. It's not a rule set in stone, but essentially, if a device is wired-in such as a smart plug, light switch, or indeed a smart light bulb from the likes of Innr, it will act as a repeater.

Battery-powered devices, such as motion and light sensors, do not tend to act as Zigbee signal repeaters - they can simply send messages to a repeater or hub.

Commercial Usage

Zigbee is used for home devices but it is also used for commercial applications as well.

Smart building solutions are a top priority for a variety of commercial industries including office, hospitality, medical, education, retail, and manufacturing. Modern smart building environments depend on many different applications and connected devices working in concert. This includes connected lighting, efficient energy control, climate and HVAC control, daylight and window blind systems, room assignment and access control, safety, and many more use cases.

Historically, most connected applications were based on proprietary, siloed and non-interoperable systems. This led to complexity, extra costs and missed opportunities to embrace the benefits of truly connected buildings.

Who uses Zigbee?

Zigbee is used by a variety of cable and telecommunication companies in their set-top boxes, satellite transceivers and home gateways to provide home monitoring and energy management products to their customers.

Zigbee is also used by vendors that provide connected lighting products for homes and businesses. With Zigbee-based smart home products, consumers can control LED figures, lightbulbs, remotes and switches in home and remotely to improve energy management.

Utility companies can use Zigbee in their smart meters to monitor, control, inform, and automate the delivery and use of energy and water. Smart meters give the consumers the information -- and automation -- needed to reduce energy use and save money.

Zigbee-based products also enhance the shopping experience for consumers by enabling faster checkouts, in-store assistance and in-store item location. Zigbee helps retailers operate more efficiently by ensuring items do not run out of stock and supporting just-in-time inventory practices, as well as monitoring temperatures, humidity, spills and so on.

Zigbee supports several devices, including intelligent shopping carts, personal shopping assistants, electronic shelf labels and asset tracking tags.

Source:

- https://zigbeealliance.org/solution/zigbee/

- https://www.the-ambient.com/guides/zigbee-devices-complete-guide-277
- https://zigbeealliance.org/market-uses/smart-home/
- https://zigbeealliance.org/market-uses/commercial/
- https://www.science.smith.edu%2F~jcardell%2FCourses%2FEGR328%2FReadings%2FZigbee%26HealthCare.pdf&usg=AOvVaw3-8NteIHvqtgrP-CTS4nZM

THE END

This is the end of the guide but not the end of your studies.

I encourage you to continue working on the 8 domains daily. Let people around you know that you are doing something important for your career and they will understand WHY you are not spending as much time with them as you used to.

If you think of anything that could be added to the guide, let me know.
Even better, take a minute to write it up and send me the update, it will be my pleasure to add it to the content and give you proper credit for it.

Best regards

Clement
The guy behind CCCure

https://cccure.education