Southern Methodist University
CS 7349/Data and Network Security
Exam #2

Name: Bingying Liang
ID: 48999397

Due: Apr 1 2024

5 essay questions (20 points each)

This document contains the questions for the exam. For your answers, create a pdf document that clearly identifies every question number and your answer to that question. Name the file containing your answers 'yourLastNameCS7349Exam1.pdf'. For example, the file for Shaibal Chakrabarty would have the name ChakrabartyCS7349Exam1.pdf. Submit your pdf file.

Answer each question fully and completely. The highlighted words are your response guide – missing them will result in points deduction. Show all of your work and state your assumptions where appropriate. The questions may have 'hints' embedded within them regarding the answer. Treat these as directions. Follow these hints as appropriate for full points.

Collaboration is expected and encouraged; however, each student must hand in their own exam. To the greatest extent possible, answers should NOT be copied but, instead, should be written in your own words. Copying answers from anywhere is plagiarism, this includes copying text directly from the textbook. Any copied answers, identical answers to other students in the course (past or present) or otherwise plagiarized answers will receive a grade of zero. More than one plagiarized answer will result in a grade of 'F' for the exam with zero points earned and the procedure for academic dishonesty will be initiated. Do not copy answers. Always use your own words. Directly under each question list all persons with whom you collaborated and list all resources used in arriving at your answer. Resources include but are not limited to the textbook used for this course, papers read on the topic, class presentations and Google search results. Note that Google is not a reference. It is a tool to find references. Don't forget to place your name in the document itself.

ALWAYS provide references, your collaborators, and submit your answers in the format of the questions, in a .pdf file. Write the question and provide the answer in the same order (numbering) as the question. Font style, type and line spacing should be the same as these intructions.

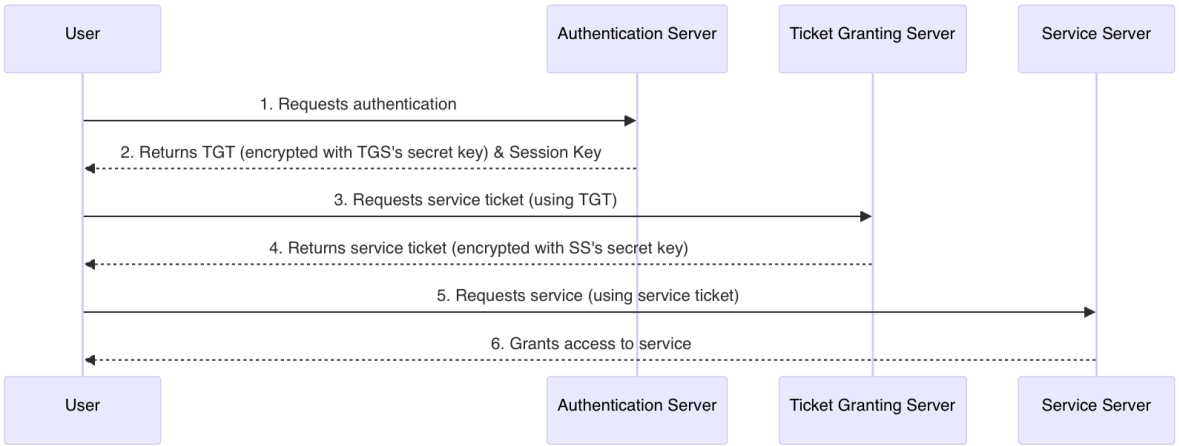
1. Kerberos is an authentication service that is often used to allow a user to gain access to a computer that is connected to the network or to establish a secure communication channel. In a MINIMUM of 1 page, explain how Kerberos works, explain why Kerberos is secure, and draw a figure that illustrates the steps involved to using Kerberos to authenticate two systems to one another while establishing a secure communication channel (where the secure communication channel uses a shared secret key). Be sure to explain each step in this symmetric session key establishment protocol.

Solution:
Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by using secret-key cryptography[1]. It is a part of the MIT Kerberos software. Here's how Kerberos works in a nutshell:

- Authentication: As for Kerberos, it employs a reliable third party referred to as Key Distribution Center (KDC) that is composed of two things – Authentication Server (AS) and Ticket Granting Server (TGS). User authenticates themselves at AS by providing a username and password.
- TGT (Ticket-Granting Ticket): After successful authentication, the AS provides the TGT and session key to the user. Encrypt TGT using TGS's secret key.
- Service Ticket: When a user wants to access a service, TGT is submitted to TGS, which then issues a service ticket for the requested service.
- Accessing the Service: The user presents the service ticket to the service server. The service server validates the ticket and grants access.

The protocol is secure because it minimizes password transmission over the network and uses time-stamped tickets to prevent replay attacks. Each step in the process is designed to ensure that the user's identity is authenticated without exposing sensitive information, and that the ticket cannot be reused by an attacker.

This diagram shows the Kerberos process [2] to the basic steps:



- User Requests Authentication: The user uses his credentials to request authentication from the authentication server (AS).
- AS Returns TGT & Session Key: AS validates the credentials and grants the ticket (TGT) and session key back to the user. TGT is encrypted using a ticket Grant server (TGS) key that cannot be decrypted by the user.
- User Requests Service Ticket: The user then uses TGT to prove their identity, thereby requesting a service ticket from TGS.
- TGS Returns Service Ticket: TGS decrypts TGT, creates a service ticket for the requested service, encrypts it with the key of the service server (SS), and then sends it to the user.
- User Requests Service: The user presents the Service ticket to SS to access the service.
- SS Grants Access: The SS decrypts the service ticket using its key, authenticates it, and then grants access to the service.

This sequence ensures that the user authenticates without having to send a password over the network again and establishes a secure communication channel with the service server using the session key.

2. Kerberos provides user authentication. The broader service in Information Security is referred to as Identity and Access Management (IAM). This is a critical service for all companies and deals with (simply put) your ability to login to the corporate network and access certain services. There are trends in IAM on-going due to multiple factors.

    a. IAM Trends/services:
        i. ITDR – Identity Threat Detection and Response
        ii. CIAM and EIAM: (Customer Identity and Access Management vs EIAM - Employee Identity and Access Management)
        iii. Passwordless Authentication (Hint: please refer to FIDO and FIDO2 standards, and include in your answers)
        iv. IGA (Identity Governance and Administration) and PAM (Privileged Access Management)
        v. Zero Trust IAM

    b. In a MINIMUM of 1 page with a diagram and/or table, please discuss the following IAM services, answering the following questions, for EACH trend:
        i. Description of the service/technology/standard
        ii. How does it differentiate from existing technology? Why was it necessary? (Hint: to improve efficiency, handle new attack vector, etc; Hint: Use a table to compare the existing with the new/add-on)
        iii. Top 2 vendors and their value proposition
        iv. Loaded question: Based on your own experience, do you think SMU uses this IAM service? Explain your answer.
    c. Note/Clarification: For EACH IAM Trend/Service in 2a, write a MINIMUM of 1 page, answering the questions of 2b. (Total 5 pages MINIMUM)

Solution:

ITDR – Identity Threat Detection and Response:

Description: Identity Threat Detection and Response (ITDR) focuses on identifying, assessing, and mitigating threats that specifically target user identities within an organization. These threats can include compromised user credentials, insider threats, and identity-based attacks that seek unauthorized access to sensitive systems and data. The core goal of ITDR solutions is to enhance an organization's security posture by providing real-time visibility of identity-related threats and providing mechanisms to respond effectively to those threats.

Key Components of ITDR:

(a) Detection: ITDR solutions employ advanced analytics, including User and Entity Behavior Analysis (UEBA), to monitor and analyze user activity across the network. By establishing a baseline of normal behavior for each identity, these systems can identify deviations that could indicate a security threat, such as compromised accounts, insider threats, or external attacks that exploit stolen credentials.

(b) Investigation: When an anomaly is detected, the ITDR system facilitates rapid investigation, providing security teams with detailed background information about suspicious activity. This may include data on related events, affected systems, and potential impacts to quickly understand the threat.

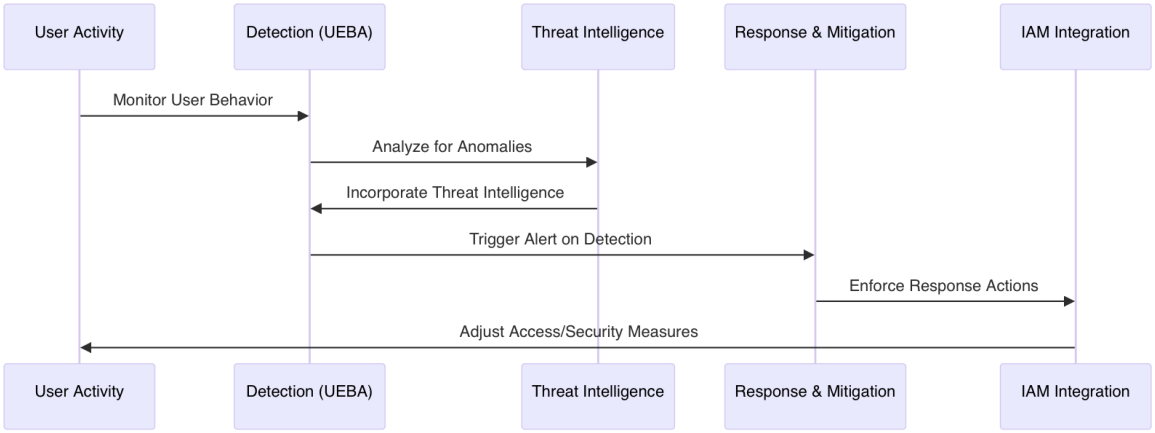
(c) Response: An effective ITDR solution not only detects and investigates threats, but also enables automated or guided responses. Depending on the severity and nature of the detected threat, responses can range from alerting security personnel, automatically revoking access, forcibly resetting passwords, or quarantinating affected systems to prevent further damage.

(d) Integration: To achieve comprehensive protection, ITDR systems are integrated with a variety of other security tools and platforms, such as SIEM (Security Information and event Management), IAM (Identity and access Management), and endpoint security solutions. This integration enables a coordinated defense strategy that leverages insights and capabilities across the security stack.

Differentiation and Necessity:

Traditional security measures often focus on perimeter defenses, ignoring the importance of protecting identity. ITDR addresses this issue by providing targeted protection for user identities, which is an important aspect given the increasing sophistication of attacks involving compromised credentials

ITDR Process Flow (Mermaid Diagram):



This diagram illustrates the continuous cycle of monitoring, detection, analysis, and response that defines the ITDR approach. It starts by monitoring user activity, analyzing their anomalies, integrating threat intelligence, and then adjusting access or security measures through IAM integration in response to detected threats.

Top Vendors and Their Value Proposition:

(a) **Microsoft Azure Active Directory Identity Protection:** Provides a comprehensive ITDR solution that integrates threat detection, risk-based conditional access, and identity protection.[3] Its value lies in its deep integration with other Microsoft security products, providing a unified approach to identity security.

(b) **Okta Identity Cloud:** Provides advanced threat detection and automatic response capabilities in its identity management services. Okta's value proposition includes ease of use, extensive integration options with other security tools, and a strong focus on user experience and security.

ITDR is an essential part of a modern cybersecurity strategy that focuses on detecting and responding to identity-related threats. By integrating with IAM systems, it provides a holistic approach to managing and protecting user identities, making it an important tool for organizations aiming to protect sensitive data and comply with regulatory standards.

SMU Usage Speculation: Given the increasing sophistication of cyber threats, SMUs are likely to leverage some form of ITDR to protect against identity theft and unauthorized access.

ii **CIAM vs. EIAM:**

Description: Customer Identity and Access Management (CIAM) and Employee Identity and Access Management (EIAM) are two key aspects of identity and access management (IAM) that address the needs of different user groups within an organization. CIAM focuses on external users, such as customers, partners or members, while EIAM focuses on internal users, primarily employees and contractors. Both frameworks are critical to managing access to applications, systems, and data, but they address different requirements and challenges.

For clarity, the information provided about CIAM and EIAM is organized into a comparison table format [6][7].

Feature Category	CIAM (Customer IAM)	EIAM (Employee IAM)
Objectives		
Scalability and Flexibility	Manage millions of identities, supporting spikes in traffic and diverse customer behaviors.	Automate access provisioning and deprovisioning to reduce IT overhead and enhance productivity.
Enhanced User Experience	Provide seamless, secure access across various digital channels to improve customer satisfaction and retention.	N/A
Privacy and Regulatory Compliance	Ensure compliance with global data protection regulations like GDPR, CCPA by managing user consents and data securely.	Secure sensitive corporate data by ensuring that only authorized employees have access, aligned with compliance requirements.
Security	Protect customer identities from fraud and breaches, employing advanced authentication and threat detection mechanisms.	Assign access rights based on employee roles, minimizing the risk of internal and external breaches.
Key Features		
Social Login and Self-Service Registration	Simplify the signup and login process.	N/A
Multi-Factor Authentication (MFA)	Enhance security without compromising user convenience.	N/A (But applicable in a broader sense for securing employee access)
Unified Customer View	Aggregate customer data across different platforms for better service and personalization.	N/A
Consent Management	Give users control over their data and comply with privacy laws.	N/A
Automated Provisioning	N/A	Streamline onboarding and offboarding processes.
Single Sign-On (SSO)	N/A (But commonly used in CIAM for user convenience)	Simplify access to multiple applications with one set of credentials.
Privileged Access Management (PAM)	N/A	Monitor and control access to critical systems and data.
Access Reviews	N/A	Regularly review and adjust access rights to ensure they are up to date.

The table makes a clear distinction between CIAM and EIAM, highlighting their respective

goals and key features. CIAM focuses on managing external user identities with an emphasis on user experience, privacy, and security, while EIAM is centered around internal employee identity management, aiming for operational efficiency, security, and compliance

Differentiation and Necessity: The distinction lies in the user base; CIAM is external (customer-focused), while EIAM is internal (employee-focused). Both are necessary for secure, efficient access management tailored to different user needs and experiences.

Top Vendors:

- CIAM - Auth0: Known for its developer-friendly platform that provides a balance between security and user experience[6].
- EIAM - IBM Security Verify: Offers a comprehensive suite for employee identity management, emphasizing security and compliance[7].

SMU Usage Speculation: SMU likely employs EIAM for internal access management, while CIAM might be used for portals accessible to students and faculty, optimizing user experience and security.

iii **Passwordless Authentication**

Description: Passwordless authentication is a security method that eliminates the need to use a password as a user identification method. Instead, it relies on other forms of verification, such as biometrics (fingerprints, facial recognition), security tokens, SMS codes, or smart cards. This approach is increasingly popular because of its ability to enhance security while providing a more user-friendly authentication experience. FIDO (Fast Identity Online) and FIDO2 are standards designed to support passwordless authentication, ensuring a secure, interoperable and flexible framework for digital authentication.

FIDO and FIDO2 Standards

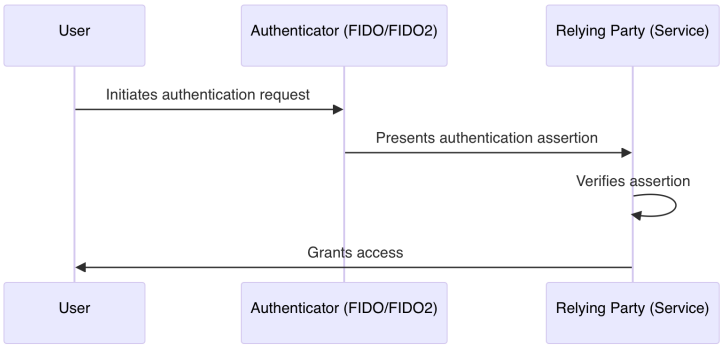
- FIDO: The FIDO[8] standard was developed by the FIDO Alliance, a consortium of technology companies that aims to reduce the world's reliance on cryptography. The FIDO specification supports password-less authentication methods that are more secure against phishing attacks and other security threats.
- FIDO2: FIDO2 extends the FIDO standard to enable users to leverage common devices as authentication factors. It includes the WebAuthn Web Authentication standard, which allows online services to use FIDO authentication through a Web browser; And CTAP Client to Authenticator Protocol, which enables external devices such as security keys or mobile phones to act as authentication factors.

Key Components

- User Device: The device that the user uses to access the service can also act as an authenticator if it has the necessary features (such as a smartphone with a fingerprint scanner).
- Authenticator: Hardware or software components that verify a user's identity (such as security keys or biometric sensors).

- Relying Party: Services that users want to access, such as websites or applications, support FIDO/FIDO2 authentication.

Passwordless Authentication Process (Mermaid Diagram)



This simplified illustration illustrates the basic flow of password-less authentication using the FIDO/FIDO2 standard. The user initiates an authentication request through the authenticator. The authenticator then presents an authentication assertion to the relying party, which verifies the assertion and grants the user access if the verification is successful.

Differentiation and Necessity: Passwords are a major security weakness. Passwordless authentication improves security and user experience by removing the risk and hassle associated with password management.

Top Vendors:

- Yubico: Offers hardware tokens for secure, passwordless access[9].
- Microsoft: Provides passwordless options through Windows Hello and Microsoft Authenticator[10].

SMU Usage Speculation: Considering the convenience and increased security, SMU may be moving towards passwordless methods for accessing campus systems.

iv IGA and PAM

Description: IGA (Identity Governance and Administration) manages digital identities and access rights, ensuring compliance and policy enforcement. PAM (Privileged Access Management) focuses on controlling access to critical systems and data by privileged users[11].

Comparative Table

Feature/Aspect	IGA	PAM
Primary Focus	Governance and administration of all digital identities	Management and security of privileged accounts
Objectives	Visibility, control, compliance, automated provisioning	Securing privileged accounts, monitoring, session management
Key Features	Access certification, role and policy management	Credential vaulting, session isolation and monitoring, least privilege enforcement
Compliance and Audit	Central to IGA objectives	Essential, with a focus on privileged account activities
Automation	Covers a broad range of identity management processes	Focuses on privileged account and access processes
User Scope	All users within the organization	Users with elevated access rights (e.g., admins, executives)

IGA and PAM address fundamental (though different) aspects of an organization's security profile. IGA provides a framework for managing and governing user access across the organization, ensuring compliance and efficient access configuration. In contrast, PAM focuses on the higher security requirements of privileged accounts, providing tools for security credulity management, session monitoring, and access control. Together, they form a powerful defense against external threats and internal risks[11].

Differentiation and Necessity: IGA provides a framework for managing identity at scale, which is critical for compliance and efficient user management. PAM addresses the specific risks of privileged access and prevents unauthorized operations on critical assets.

Top Vendors:

- SailPoint: The leader in IGA, providing visibility and control over user access.
- CyberArk: The preferred PAM solution to ensure privileged access across your organization.

SMU Usage Speculation: Smu may use IGA and PAM to manage the complex access requirements of various user groups and to protect sensitive information.

v **Zero Trust IAM**

Description: Zero Trust Identity and Access Management (IAM) is a security model that operates on the principle of "never trust, always verify." It assumes that threats can exist both outside and inside the network, so strict authentication is required for anyone trying to access a resource, regardless of where the access request comes from. This approach enhances overall security by providing access to resources based on the necessity and context of the access request, thereby minimizing the attack surface[12].

Table Comparing Traditional IAM and Zero Trust IAM

Feature	Traditional IAM	Zero Trust IAM
Trust Model	Trusts users within the network by default	Does not trust anyone by default; verifies every request
Access Control	Broad access based on user roles	Granular access based on least privilege and context
Verification Method	Often relies on single-factor authentication	Requires multi-factor authentication and continuous verification
Network Security	Focuses on securing the perimeter	Focuses on securing internal and external access points
Response to Threats	Reactive; responds after breaches are detected	Proactive; continuously monitors and adjusts access controls

Zero-trust IAM represents a strategic shift from traditional cybersecurity models, which assume that trust exists within a network. By applying the principles of minimum permissions, differentiation, and continuous verification, zero-trust IAM reduces the risk of unauthorized access and potential data breaches. Implementing a zero-trust IAM approach requires a comprehensive understanding of an organization's assets, user roles, and access requirements, and the deployment of complex technical solutions to enforce strict access control and monitoring policies

Differentiation and Necessity: Traditional security models often rely on perimeter defense. Zero-trust IAM enhances the security posture by addressing modern security challenges by assuming violations and validating every access request.

Top Vendors:

- Cisco: Provide a wide range of solutions that conform to the zero-trust model to ensure secure access across the network.
- Palo Alto Networks: Deliver comprehensive zero-trust security through its platform, focused on consistent verification and protection.

SMU Usage Speculation: As a forward-thinking university, SMU may adopt the zero-trust IAM principle to enhance security against increasingly sophisticated cyber threats.

3. In a MINIMUM of 1 page, explain how a public key cipher is typically used to provide a digital signature and explain how a user is able to authenticate a signature to verify that it came from a known individual. Be sure to include a description of how the user is able to determine the identity of the individual to whom the public key in the public key cipher is associated. Illustrate (Hint: picture) how a digital signature is used within a commonly used network communication protocol or security service. Be sure to identify the protocol or service.

Solution:

A digital signature [13] is a fundamental aspect of modern cyber security that can verify the origin and integrity of a digital message or document. A digital signature is essentially an encryption technique that mimics the properties of a physical signature, adding a layer of security that verifies the identity of the sender and ensures that the message is not altered in transit. This process utilizes the principle of public key encryption, in which a pair of keys is used: a public key that can be widely distributed and a private key that is kept secret by the owner.

How Digital Signatures Work

In the context of public key encryption, the digital signature process involves the following steps:

- Signing[14]: The sender of a message creates a hash of the message (a string of bytes of a fixed size that uniquely represents the data). The hash is then encrypted using the sender's private key, creating a digital signature. This process ensures that the signature is unique to both the document and the private key used to create the document. The original message is then sent along with the digital signature.
- Verification: Upon receiving the message and its digital signature, the recipient must verify the authenticity of the message. The recipient decrypts the digital signature using the sender's public key, revealing the original hash value created by the sender. Simultaneously, the recipient generates a new hash value from the received message. If the newly generated hash matches the one decrypted from the digital signature, it confirms that the message has not been altered and verifies the sender's identity, as only the sender's public key can decrypt the signature correctly[14].

Authentication of the Signature

To authenticate a signature and verify that it indeed came from a known individual, the recipient needs assurance that the public key used to decrypt the digital signature is genuinely associated with the sender. This association is typically established through a digital certificate, which serves as a form of digital ID card. Digital certificates are issued by trusted entities known as Certificate Authorities (CA)[14]. The certificate contains the public key and the identity of its owner, along with the digital signature of the CA, ensuring that the public key belongs to the individual or entity claimed.

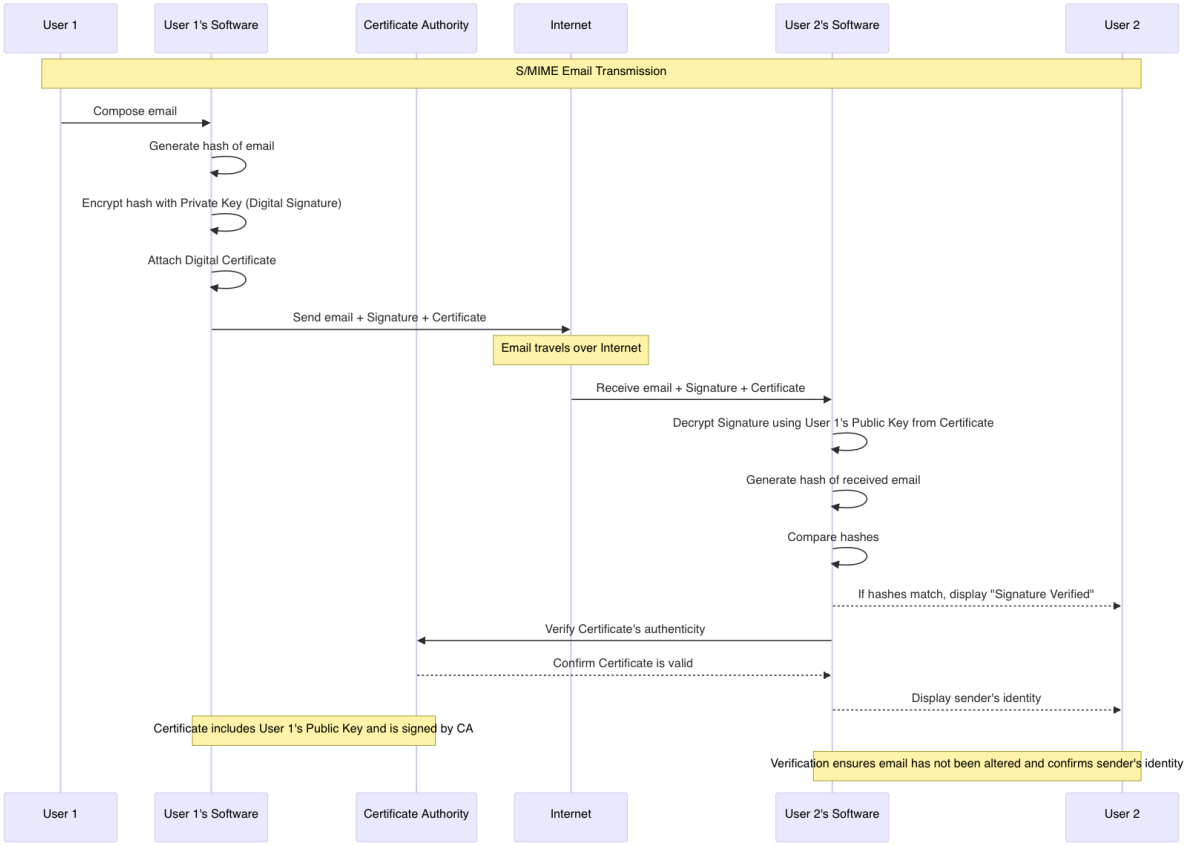
Establishing Identity The process of determining the identity associated with a public key involves:

- Certificate Verification: The recipient of a message verifies the digital certificate by using the public key of the Certificate Authority to decrypt the CA's digital signature on the certificate. If the certificate is valid, it confirms that the CA has authenticated the individual's or entity's public key.

- Trust in CAs: Trust in the digital certificate comes from the recipient's trust in the issuing CA. Operating systems and web browsers typically come preloaded with a list of trusted CAs, whose certificates are automatically trusted.

Practical Application: Secure Email (S/MIME) Secure/Multipurpose Internet Mail Extensions (S/MIME) [15] is a widely used protocol for sending digitally signed and encrypted email. S/MIME utilizes public key cryptography for both encryption and digital signatures, ensuring confidentiality, integrity, and authentication of email communications.

To illustrate the process of sending and receiving an email with S/MIME using digital signatures in a diagram, you can use Mermaid markdown. Below is a Mermaid diagram that captures the essence of this process:



This diagram explains the steps involved in sending and receiving a digitally signed email with S/MIME:

- User 1 Composes an Email: The process starts with User 1 composing an email.

- Digital Signature Creation: User 1's email software generates a hash of the email, encrypts this hash with User 1's private key (creating the digital signature), and attaches User 1's digital certificate (which contains the public key and is signed by a trusted CA).
- Sending the Email: The email, along with the digital signature and certificate, is sent over the internet to User 2.
- Receiving and Verifying the Email: User 2's software receives the email and uses the public key from User 1's certificate to decrypt the digital signature, thereby obtaining the hash of the original email. User 2's software generates a new hash based on the email received and compares it to the decrypted hash. If they match, confirm that the email was not changed during transmission and authenticate the sender.
- Certificate Verification: In addition, User 2's software verifies the authenticity of the attached certificate to the certificate authority to confirm user 1's identity.

The sequence uses the principle of public key encryption and digital certificate to ensure the integrity of the message and verify the identity of the sender.

4. The Border Gateway Protocol (BGP) is used for routing packets between Internet Service Providers (ISPs). BGP routers from each ISP communicate with one another exchanging information such as the IP addresses that are serviced within the ISP. In a MINIMUM of

   1 page, explain how BGP operates, and explain how this operation may be exploited by an adversary to allow the adversary to cause all packets destined for a particular IP address that is not serviced within the ISP to flow through that ISP. Identify and discuss at least one news article published recently that discusses victims of this type of attack.

Solution:

The Border Gateway Protocol (BGP) plays a crucial role in the operation of the Internet AS the protocol responsible for efficiently routing traffic between different autonomous systems (AS) on the Internet. Each AS represents a collection of IP networks and routers under the control of an entity (usually an ISP) that provides a common routing policy to the Internet. Essentially, BGP enables users in one part of the world to access websites and services hosted in another by determining the best path for packets to travel through a complex network of interconnected AS.

BGP hijacking occurs when an AS incorrectly declares ownership of a block of IP addresses (IP prefixes) that it does not control. This could cause Internet traffic to be rerouted through the hijackers' networks, allowing them to intercept, eavesdrop, or redirect traffic to malicious sites. BGP hijacking can be performed by taking control of or damaging BGP routers, thereby enabling attackers to advertise false routing information to the Internet[16].

The vulnerability stems from BGP's trust-based design, which assumes that all ass advertise accurate routing information. Unfortunately, this assumption makes it challenging to prevent hijacking without comprehensive monitoring and verification mechanisms in place[16] [17].

A high-profile BGP hijacking involving a Russian provider diverting traffic intended for Amazon DNS servers affected users trying to access the cryptocurrency website. This transfer enables attackers to redirect users to fraudulent websites, resulting in serious cryptocurrency theft[16].

Defending against BGP hijacking involves a variety of strategies, including IP prefix filtering (blocking traffic from known malicious networks) and AS-level BGP hijacking detection. Organizations can monitor for signs of hijacking, such as increased network latency, performance issues, and traffic routing errors. In addition, BGPsec is an extension of BGP designed to increase cryptographic security by allowing routers to sign their routing circulars, thus making unauthorized circulars easier to detect[17].

Although research and development into security enhancements such as BGPsec is ongoing, the adoption of such measures has been slow, leaving the protocol inherently vulnerable to attack. The Internet community is constantly seeking solutions that can provide more secure and verifiable routes to mitigate the risks associated with BGP hijacking[18].

BGP is a cornerstone of the Internet's infrastructure, enabling data to flow across the globe. However, its security flaws open the door to BGP hijacking, posing significant risks to data privacy, Internet reliability, and the integrity of online services. While technical solutions exist to address BGP vulnerabilities, their implementation requires global cooperation among all stakeholders in the Internet infrastructure - a challenging but necessary goal to ensure the continued growth and security of the Internet.

The BGP hijackings highlight the urgent need for improved security measures within the global Internet routing infrastructure. While solutions such as DLT and IPFS propose innovative ways to protect Internet routing and data integrity, adopting comprehensive security mechanisms remains a serious challenge for the Internet community.

5. Understanding the threat environment is critical to protecting your IT infrastructure. There are insider and outsider threats. Insider threats can be extremely damaging for exfiltrating intellectual property and sabotaging a company. You suspect someone is stealing information within your company and causing the competition to gain market share. Please find 2 companies that provide counterintelligence services to find this 'mole' inside your company.
    a. Write 1/2 page description for the services of EACH company that will help you. Total 1-page. Hint: The companies will have case studies on their websites that you can use.

    As the heat is turned on, you suspect, that external physical/cyber threats will be used to distract you from searching for this mole. Your data center, housing your IT infrastructure will be bombed. To counter this threat, you contract IBMs (or some other company) Business Continuity and Resiliency services.

    b. Write 1-page on what services IBM/other BC and Resiliency services will provide + how long the migration will take to get your network resilient. Hint: Approximate calculations will suffice – migrate 100 servers, 1000 end points, 10 enterprise applications, etc.
    c. Create a 1-page table of mitigations for the following cyberthreats, that will be unleashed on you to prevent the mole from getting caught. Explain the threat, and provide 1 threat mitigation resource (a software package, a service, a product, a configuration):
        i. RAT (Remote Access Trojan)
        ii. BotNets (Hint: look at various mutations of Mirae botnet, or any others)
        iii. Worms
        iv. Ransomware
        v. DDoS

    Hint: Create the table, with 3 columns. In the 1st column, write each threat and describe it in 3-5 lines. In the 2nd column put down the mitigation(s) of that threat, as mentioned above (a software package, a service, a product, a configuration). In the 3rd column you may give an example, write additional notes or leave it blank. Hint: Grading is always relative.

Solution:

a. Given the complexity and sensitivity of insider threats, companies need sophisticated counterintelligence services that can adapt to changing espionage strategies. International CounterIntelligence Services (ICS) and Prescient Edge are two companies that specialize in providing such services, offering comprehensive strategies to identify and neutralize insider threats.

(1) **International Counterintelligence Services (ICS)**
ICS[19] uses a multifaceted counterintelligence approach to provide services critical to identifying and neutralizing insider threats. Their products include:

- Social Engineering Defense: Customizing training and simulations to educate and test employees to recognize and respond to social engineering attacks is a common strategy for insiders to gather sensitive information.
- Technical Surveillance Countermeasures: A set of services designed to detect and eliminate electronic surveillance measures, including unauthorized listening devices or hidden cameras that could be exploited by insiders.
- Covert Internal Operations: Discreet operations are conducted within the company to identify potential breaches, gather evidence about suspected insider threats, and monitor any unauthorized access to sensitive information.
- Penetration Testing: Simulate a cyber attack on a company's network to identify vulnerabilities that could be exploited by insiders for data breaches.
- Employee Counterintelligence Monitoring: The activities of key employees are continuously monitored and monitored to detect any unusual or unauthorized behavior that could indicate an insider threat.

ICS 'approach leverages the expertise of professionals with military and government counterintelligence backgrounds to ensure a high level of security and threat detection capabilities.

(2) **Prescient Edge**
Prescient Edge's [20] counterintelligence service focuses on a wide range of threats, including those posed by insiders. The comprehensive services they offer include:

- CI Investigations & Operations: Experts analyze and investigate to identify and reduce espionage, including espionage that may be conducted by insiders.
- CI Cyber Security: Cyber defense measures specifically tailored to protect against digital espionage and insider threats, including digital forensics and cyber investigations.
- CI Collections: Activities designed to gather intelligence on potential threats to an organization, including those posed by malicious insiders.
- Insider Threat Program Development: Assistance in creating and implementing a robust insider threat program, integrating physical, organizational, and cyber security measures to protect critical assets.

By providing a broad range of counterintelligence services, Prescient Edge helps organizations protect against the complex and varied nature of insider threats.

b. **IBM Business Continuity and Resiliency Services**

IBM offers a comprehensive suite of Business Continuity and Resiliency Services designed to protect organizations against a wide range of disruptions, including cyber threats and physical damages to IT infrastructure. While direct access to IBM's page detailing these

services was restricted, based on known information about IBM's offerings in this domain, we can outline what their services likely encompass and the approximate timeline for implementing such solutions in a scenario involving the migration of 100 servers, 1000 endpoints, and 10 enterprise applications.

IBM Business Continuity and Resiliency Services[21], Services Offered in the following:

Services Offered	Description
Disaster Recovery as a Service (DRaaS)	Ensures rapid recovery of IT systems, applications, and data after a disaster using cloud technologies.
Backup as a Service (BUaaS)	Provides secure, cloud-based data backup solutions to minimize data loss.
Cyber Resilience Service	Bolsters defenses against cyber attacks to prevent, detect, and respond to threats.
IT Resilience Orchestration (ITRO)	Offers automated disaster recovery solutions for quick and efficient restoration of IT environments.
Consulting and Planning	Helps organizations develop and refine their business continuity plans for comprehensive protection.

Implementing IBM's Business Continuity and Resiliency Services for a company with 100 servers, 1000 endpoints, and 10 enterprise applications involves several key phases:

Phase	Duration	Description
Assessment and Planning	1-2 weeks	Initial consultations to understand needs, identify critical systems and data, and plan strategies.
Solution Design and Setup	4-6 weeks	Design disaster recovery and continuity solutions, including cloud backup and cybersecurity measures.
Migration and Implementation	6-8 weeks	Migrate data, set up replication for servers and endpoints, and configure disaster recovery.
Training and Optimization	2-4 weeks	Train IT staff and optimize solutions based on performance and recovery tests.

Total Estimated Time: 13-20 weeks.

This timeline is an approximation and could vary based on the complexity of the organization's IT infrastructure, the specific solutions chosen, and the level of customization required. IBM's approach emphasizes minimizing downtime and ensuring that organizations

can quickly resume operations after a disruption, with a focus on not just recovery, but also on strengthening defenses against future threats.

c. **Cyberthreat Mitigations Table Expanded**

For a more comprehensive mitigation strategy against specific cyberthreats[22][23]:

Cyberthreat	Mitigation Resource	Example/Notes
Remote Access Trojan (RAT)	Security awareness training, strict access control, secure remote access solutions, and implementing least privilege.	Imperva highlights the importance of vigilance against RATs due to their stealthy nature and ability to give attackers administrative control over a victim's computer. Tools like Imperva's Web Application Firewall can prevent such attacks by monitoring and blocking malicious traffic.
BotNets	Intrusion Detection Systems (IDS) like Snort, and Mail Assure for email security.	Snort is used industry-wide for its packet sniffing functions and anomaly- and signature-based policies that can flag several potential security threats, including those related to botnets. Mail Assure provides advanced threat protection for inbound and outbound emails, reducing the risk of malware attacks delivered via email.
Worms	Use of comprehensive antivirus solutions and regular patching of systems.	Antivirus solutions can detect and remove worms. Regular system updates and patches close vulnerabilities that worms might exploit to spread.
Ransomware	Backup solutions and advanced threat protection systems.	Regular backups ensure data can be restored without paying ransoms. Advanced threat protection systems can detect and block ransomware before it encrypts files.
DDoS	DDoS protection services like Cloudflare or Akamai.	These services can absorb and mitigate large-scale DDoS attacks, preventing them from overwhelming your network.

Each of these mitigation resources plays a critical role in a layered security strategy designed to defend against a range of cyber threats, including those that may be part of an effort to distract from or facilitate insider threats. By implementing these solutions, organizations can better protectagainst a wide array of cyber threats.

References

[1] 'Kerberos: The Network Authentication Protocol'. Accessed: Mar. 17, 2024. [Online]. Available: http://web.mit.edu/kerberos/

[2] W. Stallings, Cryptography and Network Security: Principles and Practice, 0008 ed. Pearson, 2020.

[3] 'Identity Threat Detection and Response (ITDR) — Microsoft Security'. Accessed: Mar. 18, 2024. [Online]. Available: https://www.microsoft.com/en-us/security/business/solutions/identity-threat-detection-response

[4] 'Identity Threat Detection and Response (ITDR) Explained', crowdstrike.com. Accessed: Mar. 18, 2024. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/identity-security/identity-threat-detection-and-response-itdr/

[5] 'What Is Identity Threat Detection & Response (ITDR)? — Proofpoint US', Proofpoint. Accessed: Mar. 18, 2024. [Online]. Available: https://www.proofpoint.com/us/threat-reference/identity-threat-detection-and-response-itdr

[6] Auth0, 'Get Started', Auth0 Docs. Accessed: Mar. 19, 2024. [Online]. Available: https://auth0.com/docs/

[7] rolyon, 'Microsoft Entra ID documentation - Microsoft Entra ID'. Accessed: Mar. 19, 2024. [Online]. Available: https://learn.microsoft.com/en-us/entra/identity/

[8] 'FIDO Alliance', FIDO Alliance. Accessed: Mar. 19, 2024. [Online]. Available: https://fidoalliance.org/?lang=zh-hans

[9] 'Yubico Developers'. Accessed: Mar. 19, 2024. [Online]. Available: https://developers.yubico.com/

[10] 'Microsoft Entra passwordless sign-in - Microsoft Entra ID — Microsoft Learn'. Accessed: Mar. 19, 2024. [Online]. Available: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless

[11] J. T. Force, 'Security and Privacy Controls for Information Systems and Organizations', National Institute of Standards and Technology, NIST Special Publication (SP) 800-53 Rev. 5, Dec. 2020. doi: 10.6028/NIST.SP.800-53r5.

[12] 'Zero Trust Model - Modern Security Architecture — Microsoft Security'. Accessed: Mar. 19, 2024. [Online]. Available: https://www.microsoft.com/en-us/security/business/zero-trust

[13] 'Digital signature', Wikipedia. Mar. 13, 2024. Accessed: Mar. 18, 2024. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Digital_signature&oldid=1213566487

[14] 'What Are Digital Signatures And How Do They Work', Sectigo® Official. Accessed: Mar. 18, 2024. [Online]. Available: https://www.sectigo.com/resource-library/how-digital-signatures-work

[15] J. Watson, 'What is public key cryptography, how does it work and what are its uses?', Comparitech. Accessed: Mar. 18, 2024. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/what-is-public-key-cryptography/

[16] 'What is BGP hijacking?' Accessed: Mar. 18, 2024. [Online]. Available: https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/

[17] ‘How does BGP hijacking work and what are the risks? — TechTarget’, Security. Accessed: Mar. 18, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/How-does-BGP-hijacking-work-and-what-are-the-risks

[18] ‘CertiK - BGP Hijacking: How Hackers Circumvent Internet Routing Security to Tear the Digital Fabric of Trust’. Accessed: Mar. 18, 2024. [Online]. Available: https://certik.com/resources/blog/bgp-hijacking-how-hackers-circumvent-internet-routing-security-to-tear-the

[19] ‘Counterintelligence Services - ICSWorld™ Since 1967’. Accessed: Mar. 18, 2024. [Online]. Available: https://www.icsworld.com/Private_Investigation_Services/Counterintelligence_Services.aspx

[20] ‘Intelligence Support’, Prescient Edge. Accessed: Mar. 18, 2024. [Online]. Available: https://www.prescientedge.com/our-services/intelligence-support/

[21] ‘Security and resiliency services — IBM’. Accessed: Mar. 18, 2024. [Online]. Available: https://www.ibm.com/consulting/business-continuity

[22] ‘Imperva Web Application Firewall (WAF) — App & API Protection’, Products. Accessed: Mar. 18, 2024. [Online]. Available: https://www.imperva.com/products/web-application-firewall-waf/

[23] ‘Software Reviews, Opinions, and Tips - DNSstuff’, Software Reviews, Opinions, and Tips - DNSstuff. Accessed: Mar. 18, 2024. [Online]. Available: https://www.dnsstuff.com/