Cloud Computing

MUCPD – DSIC - UPV

Cloud Security Fundamentals

Overview

- What is Cloud Security?
  - Protection of data, services and infrastructure
- Why Cloud security is critical
  - Growing reliance on cloud services
  - Wide exposure
- Goals of this session
  - Gain a good understanding of cloud security principles
  - Explore advanced strategies and best practices
  - Learn about tools and frameworks

Evolution of cloud security

- Traditional security models
  - Perimeter-based defenses
- Shift to cloud-centric security approaches
  - Emphasis on data and identity security
  - Cloud-native security tools
- Zero-trust Security model
  - Never trust always verify
  - Continuous authentication and authorization
- Integration of devops for security
  - Automation
- Impact of regulations
  - GDPR, HIPAA, PCI DSS,…

The shared responsibility model

- Clarifies security responsibilities
- Cloud provider responsibilities
  - Cloud infrastructure
  - Users can provision resources without human interaction
- Customer’s responsibilities
  - Data, applications, OS, configurations,…
- Variations by service model
- Implications
  - Importance of understanding boundaries
  - Collaboration with providers for comprehensive approach

Identity and Access Management (IAM)

- Framework for managing digital identities and access to resources
- Core components:
  - Authentication
  - Authorization
- Importance of IAM
  - Prevents unauthorized access
  - Protects sensitive data and resources
- Challenges in cloud environments
  - Scalability and complexity
  - Managing diverse user groups and access needs

Authentication

- Authentication methods
  - Passwords and passphrases
    - Complexity requirements
  - Biometric authentication
    - Fingerprints, facial recognition, iris, …
  - Token-based authentication
    - One-time passwords, smart cards, …

Authorization

- Authorization models
  - Role based access control (RBAC)
    - Assigning permissions to roles
  - Attribute-based access control (ABAC)
    - Policies based on user attributes
  - Policy-based access control (PBAC)
    - Centralized policy management

Federation

- Single Sign-On (SSO)
    - Streamlined access across multiple systems
- Trust relationships
    - Between identity providers (IdP) and service providers
- Capabilities
    - Tokens encoding authorization for holder

Challenges

- Complexity vs security
  - Balance user convenience vs security risks
- Integration with legacy systems
  - Adapting modern IAM to existing infrastructures

Multi Factor authentication (MFA)

- **Importance**
  - **Adds layers of security**
  - **Reduces the risks of credentials compromise**
- **Types of authentication factors**
  - **Something you know:** pins**,…**
  - **Something you have:** tokens, smart cards, …
  - **Something you are:** biometrics

Implementing MFA

- Strategies
  - Risk-based authentication
    - Adjusts requirements based on risk levels
  - Adaptive authentication
    - Context-aware authentication decissions
- Integration considerations
  - Compatibility with existing systems
  - User experience and adoption
- Best practices
  - Enforce MFA for privileged accounts
  - Regularly review authentication methods

Data Encryption techniques

- Why encrypt?
  - Protects confidentiality and integrity
    - Helps comply with regulations
- Types of encryption
  - Symmetric encryption
    - Single key for encryption/decryption (e.g., AES, DES)
  - Asymmetric encryption
    - Public and private key pairs (e.g., RSA, ECC)

Encryption in the cloud

- Data at rest
  - Disk encryption, database encryption
    - Helps protect from unadvertant leaks
- Data in transit
  - TLS/SSL protocols
    - Helps protect integrity and privacy
    - Protects against MITM attacks

Key Management Systems (KMS)

- What is KMS?
  - System for managing cryptographic keys
- Key lifecycle management
  - Generation
  - Distribution
  - Storage
  - Rotation
  - Revocation

Key Management Systems (KMS)

- Key hierarchies and Wrapping
  - Master keys encrypt data keys
    - Adds layers of security
    - Similar in many ways to how TSL works
- Integration with cloud services
  - Automates encryption tasks
    - Centralizes key management

KMS Benefits

- Enhances security through proper key handling
- Simplifies key management processes
- Supports compliance requirements

KMS Best practices and challenges

- **Best practices**
  - **Access controls:** restrict key usage permissions
  - **Separation of duties:** divide key management tasks
  - **Audit logging:** Monitor key usage and administrative actions
  - **Key rotation policies:** regularly update keys
- **Challenges**
  - **Managing keys across multiple environments**
  - **Ensuring availability and performance**

Data Loss Prevention (DLP)

- **Purpose**
  - **Prevent unauthorized data disclosure**
  - **Ensure compliance with data protection laws**
- **Key components**
  - **Data discovery:** identify sensitive data.
  - **Data classification:** categorize data by sensitivity
  - **Policy enforcement:** control data access and movement
  - **Monitoring and reporting:** track data usage
- **Types of DLP**
  - **Endpoint DLP:** controls on user devices
  - **Network DLP:** Monitors data in motion
  - **Cloud DLP:** protects data in cloud services

DLP in the Cloud

- Integration with cloud services
  - Use APIs and cloud native tools
- Encryption and tokenization
  - Masking sensitive data elements
- User behavior analytics
  - Detecting insider threats and anomalies
- Challenges
  - Balancing security with user productivity
  - Managing false positives/negatives
- Best practices
  - Employee training and regular audits

Securing Cloud Infrastructure: Compute

- Instance hardening
  - Disable unnecessary services/daemons
  - Apply diligently security patches
- Secure configuration management
  - Ensure security baselines. Automate.
- Access control mechanisms
  - Implement ssh key management
  - Use bastion hosts for admin access
- Virtualization Security
  - Ensure isolation between VMs

Securing Cloud Infrastructure: Storage

- Access controls
  - Fine grained permissions
  - Identity-based policies
- Encryption at rest
  - Both client-side or server-side
- Data Replication and Backup
  - Implement versioning
- Data lifecycle management
  - Automate data retention and deletion policies

Securing Cloud Infrastructure: Networking

- Virtual Private Clouds (VPC)
  - Isolate resources in private networks
- Security groups – Network ACLs
  - Control inbound and outbound traffic
- Network traffic encryption
  - Through VPN and TLS protocols. Zero trust networks.
- Monitoring and intrusion detection
  - Through traffic analysis tooling

Application security: Development

- **Secure software development lifecycle (SSDLC)**
  - **Integrate security at each development phase**
- **Secure coding practices**
  - **Input validation, error handling, avoid hard-coded creds**
- **Security testing tools**
  - **SAST:** Static code analysis
  - **DAST:** Dynamic testing in runtime
  - **IAST:** Interactive testing, combining SAST and DAST
  - **SCA:** Analyze third party components

Application security: Deployment

- Secure configurations
  - Follow hardening recomendations
- Secrets management
  - Avoid exposing secrets in the clear when deploying
- Continuous monitoring
  - Detect anomalous client behaviors

Compliance and legal considerations

- Understand regulations
  - Hire expertise…
- Compliance frameworks
  - NIST, ISO 27001, ISA CCM, Esquema Nacional de Seguridad…
- Data residence and sovereignty
  - Where data is determines what laws it is subject to
- Cloud provider compliance
  - Piggyback on top of it
- Auditing/reporting
  - Prepare for compliance audits/maintain needed records

Incident Response

- **Minimize impact of security breaches**
- **Incidence response plan**
  - **Preparation:** Roles and responsibilities
  - **Detection and analysis:** Monitoring and threat intel
  - **Containment, Eradication, Recovery**
    - **Limit damage, remove threats, restore systems**
  - **Post-Incident activities:** Lessons learned

- **Tools & Tech**
  - **SIEM, SOAR, forensic tools**

Incident Response: Challenges

- Limited visibility in the cloud
  - Remoteness does not help
  - Provider also gets relevant data
  - Provider must be involved
- Best practices
  - Periodic revisions
  - Establish cooperation plan with provider

Automation

- Benefits: less errors, higher reliability
  - Speed and efficiency
  - Consistency in security practices
- Infrastructure as Code (IaC)
  - Automate deployment of secure configurations
- Security Orchestration, Automation, and Response (SOAR)
  - Integrate diverse tools within complex automated workflows
- Automate compliance monitoring
  - Continuous compliance checks, help ensure compliance…

Emerging threats in cloud security

Concept: Attack Surface

- Supply chain attacks
  - Compromised third party components
- Advanced persistent threats (APTs)
  - Sophisticated long term attacks
- Cloud misconfigurations
  - Common cause of breaches
- Container and Kubernetes vulnerabilities
  - Exploits in container environments
- IoT and Edge Computing Risks
  - Exploits in container environments

Cloud security frameworks

- Cloud Security Alliance (CSA)
  - Cloud controls matrix (CCM)
- NIST Guidelines
  - Best practices in risk management
- ISO/IEC Standards
  - 27017 and 27018 for cloud services
- CIS benchmarks
  - Configuration guidelines
- Benefits
  - Compliance alignment
  - Standardization

Some case studies

- Case study 1: Capital One breach
- Case study 2: Dropbox password leak
- Case study 3: Tesla Kubernetes exploit
- Key takeaways

Capital One Data Breach Overview

- **Incident summary**
  - **Breach exposed personal data of over 100 M customers**
  - **Names, addresses, credit scores, SSNs, etc,…**
- **Timeline**
  - **March 2019:** Data accessed by attacker
  - **July 2019:** Breach discovered and publicly disclosed
  - **July 2019:** Arrest by FBI

Causes of the breach

- Misconfigured Web Application Firewall (WAF)
  - Exploited SSRF vulnerability
  - Accessed AWS EC2 metadata service
- Overly permissive IAM Role Permissions
  - Excessive privilege granted
  - Violated least privilege principle
- Ineffective network segmentation
  - Inadequate isolation of sensitive data
- Insufficient monitoring and logging
  - Delayed detection of unauthorized access
  - Lack of anomaly detection mechanisms

Remedies applied by Capital One

- Immediate fixes
  - Corrected WAF configuration
  - Revoked compromised credentials
- Enhanced access controls
  - Tightened IAM policies
    - Implemented least privileged access
- Improved network security
  - Strengthened network segmentation
  - Updated firewall rules
- Advanced monitoring
  - Deployed AWS GuardDuty
    - Enabled detailed logging and anomaly detection

Lessons from Capital One breach

- Enforce Least Privilege principle -- ALWAYS
    - Limit permissions to essential functions
- Secure configuration management
    - Regularly and validate settings
        - Implemented least privileged access
- Pay attention to monitoring and detection
    - Use tooling for real time alerts
- Training
    - Staff must be security savvy

Impact on Capital One

- Financial penalties
  - $80 Million fine
- Legal actions
  - Class action lawsuits
- Reputational damage
  - Loss of customer trust
- Operational costs
  - Expenses for remediation and notifications

Dropbox Password leak Overview

- **Incident summary**
  - **Exposed credentials of over 68 million users**
  - **Names, addresses, credit scores, SSNs, etc,…**
- **Timeline**
  - **2012:** Breach occurred via compromised employee account
  - **2016:** Full public disclosure

Causes of the breach

- Compromised employee credentials
  - Password reuse lead to unauthorized access
- Weak password hashing
  - SHA-1 without salting
- Insufficient access controls
  - Overprivileged employee account
  - Lack of multi factor authentication

Remedies applied by Dropbox

- Password resets and notifications
  - Mandatory password changes for affected users
- Enhanced authentication
  - Implemented MFA for users and employees
- Improved password storage
  - Switched to bcrypt with salting
- Access control review
  - Enforced role based
- Security infrastructure enhancements
  - Deployed anomaly detection systems

Lessons from Dropbox breach

- Enforce strong authentication
  - Implement MFA to secure accounts
- Secure password handling
  - Use strong hashing algorithms with salting
- Avoid credentials reuse
  - Education…
- Apply Least Privilege
- Timely disclosure
  - Inform users promptly, so they can take proper action

Impact on Dropbox

- User trust erosion
  - Customers questioned data security
- Competitive disadvantage
  - Potential loss of customers to competition
- Regulatory scrutiny
  - Increased attention on data protection practices

Tesla Kubernetes Exploit

- **Incident summary**
  - **Attackers used unsecured Kubernetes console**
  - **Performed cryptojacking using Tesla's resources**
- **Timeline**
  - **February 2018:** Breach discovered by RedLock

Causes of the Tesla breach

- Unsecured Kubernetes Console
  - No authentication was required
- Exposure of AWS credentials
  - Hardcoded credentials in Kubernetes PODs
- Inadequate network controls
  - Publicly accessible critical systems
- Insufficient monitoring
  - Lack of resource usage and anomaly detection

Remedies applied by Tesla

- Secured Kubernetes console
  - Enabled authentication and RBAC
- Improved secrets management
  - Removed hardcoded credentials
  - Used Kubernetes secrets for sensistive data
- Enhanced network security
  - Applied network policies and firewalls
- Implemented monitoring systems
  - Deployed IDS and resource monitoring
- Introduced security assessments
  - Regular vulnerability scans

Lessons from Tesla breach

- Secure default configurations
  - Always configure authentication for admin interfaces
- Effective secrets management
  - Store credentials securely
- Network segmentation
  - Restrict access to critical systems
- Continuous monitoring
- Regular security assessments
  - Inform users promptly, so they can take proper action

Impact on Tesla

- Operational cost
  - Unauthorized resource consumption
- Potential data exposure
  - Risk of sensitive data being accessed
- Reputational risk
  - Public perception affected

Key takeaways

- Misconfiguration poses risks
  - Secure configurations are critical
- Access control is critical
  - Enforce least privileges and proper permissions
- Secrets management matters
  - Protect sensitive information diligently
- Monitoring is essential
  - Implement robust detection systems
- Timely response
  - Quick detection and remediation reduce impact
- Human factors
  - Train on security best practices

Strengthening Cloud Security

- Proactive measures
  - Prevent incidents through strong security attitude
- Continuous improvement
  - Regularly update and test security strategies
- Collaboration
  - Foster a culture of security across the org
- Leverage tools and expertise
  - Use available resource to enhance protection