|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aspect** | **Model** | **TLS (Transport Layer Security)** | **IPsec (Internet Protocol Security)** | **DNSSEC (Domain Name System Security Extensions)** |
| **Main Threats** | **STRIDE** | - **Spoofing**: Attacker impersonates trusted servers by exploiting certificate vulnerabilities. | - **Spoofing**: Attacker intercepts or impersonates IP addresses. | - **Spoofing**: Quantum-compromised DNSSEC signatures allow attackers to fake DNS responses. |
|  | . | -**Tampering**: Unauthorized modification of data in transit by exploiting weak encryption | -**Tampering**: Altering IP packets after decryption by breaking IPsec encryption. | -**Tampering**: Alteration of DNS records due to compromised signatures. |
|  |  | - **Repudiation**: Quantum threats to digital signatures lead to denial of actions. | -**Repudiation**: IPsec lacks strong non-repudiation due to its encryption-based authentication vulnerabilities under quantum attacks. | **-Repudiation**: Forged DNSSEC signatures make it difficult to verify authentic responses. |
|  |  | -**Denial of Service (DoS)**: Overhead from quantum-safe encryption makes TLS susceptible to DoS. | -**DoS**: Resource demands for quantum-safe algorithms increase vulnerability to service disruptions. | -**DoS**: Increased processing for quantum-safe DNSSEC signatures makes DNS servers vulnerable to DoS. |
|  |  | - **Elevation of Privilege**: Breaking TLS credentials could enable unauthorized control over data. | - **Elevation of Privilege**: Quantum-decrypted keys allow unauthorized network access. | -**Elevation of Privilege**: Compromised DNSSEC records can enable unauthorized access to various services. |
| **Threat Identification Focus** | **STRIDE** | Emphasis on classifying high-level threats (Spoofing, Tampering, etc.) across the TLS handshake, encryption, and certificate validation. | Focuses on spoofing, packet integrity, and data exposure risks without simulating detailed scenarios. | Identifies potential threats (e.g., DNS spoofing, tampering) but without extensive technical context on DNSSEC operations. |
|  | **PASTA** | Detailed threat analysis, including technical and business perspectives, evaluating quantum vulnerabilities in TLS key exchange. | Extensive threat assessment focused on IPsec encryption weaknesses, quantum-safe protocol transitions, and impact on VPN integrity. | In-depth threat analysis of DNSSEC’s risks under quantum decryption, including DNS record spoofing and data tampering scenarios. |
| **Business Objective** | **STRIDE** | Ensure safe user transactions, protect data privacy, and maintain business reputation by preventing TLS protocol compromise. | Safeguard corporate communications via VPNs and secure data exchanges to comply with regulations and maintain business continuity. | Prevent DNS tampering that could redirect customers to phishing sites or compromise business integrity. |
|  | **PASTA** | Maintain trust and continuity in secure customer interactions, safeguarding against data breaches with quantum-safe protocols. | Secure sensitive business communications, prevent data breaches, and maintain regulatory compliance by implementing secure IPsec. | Ensure DNS authenticity to protect users from spoofed DNS records and phishing threats, thereby maintaining service reliability. |
| **Technical Objective** | **STRIDE** | Encrypt communications, validate certificates, and authenticate server-client interactions to prevent unauthorized access. | Provide confidentiality, data integrity, and authentication through secure IPsec tunnels and encrypted communication. | Ensure data integrity of DNS records through cryptographic signatures, secure DNS responses against tampering and spoofing. |
|  | **PASTA** | Quantum-resilient encryption and hybrid methods for TLS; ensure that legacy systems can support secure communication transitions. | Quantum-resistant key exchanges for IPsec with minimal latency, and secure VPN channels for internal business communication. | Migrate DNSSEC to quantum-safe signatures, improve the DNS infrastructure to handle additional processing overhead from new algorithms. |
| **Scope** | **STRIDE** | TLS components: handshake, symmetric/asymmetric encryption algorithms, certificates, and key exchanges. | IPsec protocols: Authentication Header (AH), Encapsulating Security Payload (ESP), key exchange protocols, encryption mechanisms. | DNSSEC: DNS records, digital signatures, DNS resolvers, and zone files. |
|  | **PASTA** | Detailed components analysis, TLS handshake simulation, certificate management,encryption transitions to quantum-safe algorithms. | Complete IPsec architecture, including session establishment, tunnel management, and encrypted packet analysis. | DNSSEC’s entire framework, including DNS records, resolvers, cryptographic key management, and recursive and authoritative servers. |
| **Threat Intelligence** | **STRIDE** | Identifies certificate vulnerabilities, DoS risks from certificate spoofing, and MITM (Man-in-the-Middle) threats in quantum scenarios. | Focuses on quantum vulnerabilities in key exchange, IP packet tampering, and spoofing through compromised authentication. | Emphasizes quantum threats to DNSSEC’s signatures, risks of spoofing, and tampering attacks on DNS integrity. |
|  | **PASTA** | Quantum decryption risks in RSA/Diffie-Hellman, increasing risk of MITM attacks and certificate spoofing. | Quantum threats to IPsec’s AES and RSA-based methods for data exchange; detailed scenarios of packet sniffing and spoofing. | Advanced DNSSEC scenarios, such as quantum-enabled phishing, DNS tampering, and MITM attacks that compromise DNS records. |
| **Attack Simulation** | **STRIDE** | Theoretical classification of threats to data confidentiality, encryption breakage, and identity spoofing in TLS sessions**.** | Identifies IPsec’s susceptibility to spoofing and MITM attacks; emphasizes risks without in-depth attack analysis. | Basic DNSSEC attack possibilities like spoofing, data tampering, and key compromise without in-depth scenario analysis. |
|  | **PASTA** | Detailed attack scenarios include quantum MITM attacks, certificate impersonation, and session decryption for data breach simulations. | Simulates quantum MITM, packet sniffing, and IP packet tampering due to quantum-decrypted IPsec protocols and keys. | Detailed simulations for DNSSEC attacks including spoofed DNS responses, redirection to malicious sites, and compromised DNS records. |
| **Main Threats in PASTA** | **PASTA** | -**Business Disruption**: Data breaches and exposure of client data disrupt business operations. - **Unauthorized Access**: Quantum-cracked certificates enable attackers to intercept TLS traffic. - **Data Leakage**: Sensitive information exposed through decrypted sessions. - **Data Integrity**: TLS session tampering through forged certificates. - **Reputational Risk**: Customer trust erosion due to data exposure or MITM attacks. | -**Business Disruption**: Compromise of VPNs and secure IP-based communications. - **Unauthorized Access**: IP spoofing and network access due to compromised IPsec keys. - **Data Leakage**: Business-sensitive data is accessible through decrypted IPsec packets. - **Data Integrity**: IP packet modification by attackers. - **Reputational Risk**: Loss of trust in secure communications and potential regulatory breaches. | -**Business Disruption**: Redirected traffic damages user trust and interrupts business services. - **Unauthorized Access**: Spoofed DNS responses allow attackers unauthorized control. - **Data Leakage**: DNS records and queries exposed without encryption. - **Data Integrity**: DNS record tampering leading to compromised user data. - **Reputational Risk**: Redirecting users to phishing sites harms brand image. |
| **Risk and Impact Analysis** | **PASTA** | - **Business Disruption**: Data breaches and exposure of client data disrupt business operations. - **Unauthorized Access**: Quantum-cracked certificates enable attackers to intercept TLS traffic. - **Data Leakage**: Sensitive information exposed through decrypted sessions. - **Data Integrity**: TLS session tampering through forged certificates. - **Reputational Risk**: Customer trust erosion due to data exposure or MITM attacks. | - **Business Disruption**: Compromise of VPNs and secure IP-based communications. - **Unauthorized Access**: IP spoofing and network access due to compromised IPsec keys. - **Data Leakage**: Business-sensitive data is accessible through decrypted IPsec packets. - **Data Integrity**: IP packet modification by attackers. - **Reputational Risk**: Loss of trust in secure communications and potential regulatory breaches. | - **Business Disruption**: Redirected traffic damages user trust and interrupts business services. - **Unauthorized Access**: Spoofed DNS responses allow attackers unauthorized control. - **Data Leakage**: DNS records and queries exposed without encryption. - **Data Integrity**: DNS record tampering leading to compromised user data. - **Reputational Risk**: Redirecting users to phishing sites harms brand image. |
| **Risk and Impact Analysis** | **STRIDE** | Risks of data theft, customer loss, regulatory penalties, reputation damage from data breaches or MITM attacks on TLS. | Potential loss of internal information, business disruption, fines, and breaches in sensitive communication from IPsec compromise. | Risks of brand damage, financial loss, and user harm from DNSSEC failure, including phishing or redirect attacks. |
|  | **PASTA** | Evaluates regulatory, financial, and reputation damage; calculates potential losses due to customer data breaches under quantum risks. | Quantifies financial and operational impact of compromised IPsec sessions, regulatory implications of data breaches. | Business and operational impact from DNS tampering attacks, including reputation harm and increased risk of phishing for users. |
| **Mitigation Strategies** | **STRIDE** | - Transition to quantum-safe encryption (e.g., lattice-based, hash-based). - Increase monitoring for suspicious connections. | - Migrate to quantum-resistant key exchange protocols. - Use traffic analysis to monitor for IPsec-based spoofing and tampering. | - Implement quantum-safe DNSSEC signatures (e.g., hash-based). - Enhance DNS infrastructure to handle quantum-safe overhead. |
|  |  | - Employ hybrid encryption to maintain backward compatibility. - Strengthen DoS resilience through resource allocation. |  |  |
|  | **PASTA** | - Review and update TLS security policies. - Conduct post-incident reviews for TLS. | - Review IPsec security policies regularly. - Conduct post-incident analysis for breaches. | - Review DNSSEC policies regularly. - Conduct post-incident reviews for DNSSEC. |
|  |  | - Review and update TLS security policies. - Conduct post-incident reviews for TLS. | - Review IPsec security policies regularly. - Conduct post-incident analysis for breaches. | - Review DNSSEC policies regularly. - Conduct post-incident reviews for DNSSEC. |