**3-4 protocols and implement them using both the STRIDE and PASTA models**.

### Recommended Protocols

1. **TLS (Transport Layer Security)** – Critical for secure communications.
2. **IPsec (Internet Protocol Security)** – Provides security at the Internet layer.
3. **OAuth** – Common for authorization, especially in applications.
4. **DNSSEC** – Adds security to DNS, a foundational service.

### Applying STRIDE

The STRIDE model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) can identify potential threats for each protocol:

**TLS**:

* 1. **Spoofing**: Examine if an attacker can impersonate a secure endpoint.
  2. **Tampering**: Assess risks of data alteration during transmission.
  3. **Repudiation**: Investigate ways to verify transactions for non-repudiation.
  4. **Information Disclosure**: Identify sensitive data potentially exposed.
  5. **Denial of Service**: Determine the potential for TLS-based service interruptions.
  6. **Elevation of Privilege**: Assess risks of unauthorized access escalation.

**IPsec**:

* 1. **Spoofing**: Analyze vulnerability to IP spoofing attacks.
  2. **Tampering**: Assess data integrity mechanisms to detect unauthorized changes.
  3. **Repudiation**: Explore traceability in secure communications.
  4. **Information Disclosure**: Identify risks to confidential IP data.
  5. **Denial of Service**: Check for service interruption vulnerabilities.
  6. **Elevation of Privilege**: Look into IPsec's privilege escalation protections.

**OAuth**:

* 1. **Spoofing**: Risk of malicious actors impersonating a user or service.
  2. **Tampering**: Examine token integrity against modification.
  3. **Repudiation**: Token non-repudiation for accountability.
  4. **Information Disclosure**: Risk of exposing sensitive user data.
  5. **Denial of Service**: Susceptibility to token-based service interruptions.
  6. **Elevation of Privilege**: Potential for unauthorized privilege escalation.

**DNSSEC**:

* 1. **Spoofing**: Address risks of DNS impersonation.
  2. **Tampering**: Focus on data integrity to prevent unauthorized alterations.
  3. **Repudiation**: Validate logs to ensure activity tracking.
  4. **Information Disclosure**: Risk of revealing DNS query data.
  5. **Denial of Service**: Identify potential DNSSEC-induced service disruptions.
  6. **Elevation of Privilege**: Protection against unauthorized elevation within DNS zones

### Applying PASTA

The PASTA model (Process for Attack Simulation and Threat Analysis) provides a risk-centric framework for each protocol:

**TLS:**

* 1. **Define Objectives**: Secure data transmission.
  2. **Define Technical Scope**: Focus on encryption, decryption, and authentication.
  3. **Threat Intelligence**: Quantum risk to public-key cryptography.
  4. **Vulnerability Analysis**: Weaknesses in legacy encryption standards.
  5. **Threat Modeling**: Identify key assets (data in transit) and attack vectors.
  6. **Risk Analysis & Evaluation**: Assess attack feasibility and impact.
  7. **Security Controls**: Implement quantum-safe algorithms.

**IPsec**:

* 1. **Define Objectives**: Ensure IP-level data security.
  2. **Define Technical Scope**: Encryption and authentication in IP layer.
  3. **Threat Intelligence**: Quantum threats to IPsec’s public-key systems.
  4. **Vulnerability Analysis**: Analyze tunnel and transport mode encryption.
  5. **Threat Modeling**: Identify IPsec assets (network traffic) and entry points.
  6. **Risk Analysis & Evaluation**: Evaluate potential compromise scope.
  7. **Security Controls**: Update to quantum-resistant encryption.

**OAuth**:

* 1. **Define Objectives**: Secure authorization across services.
  2. **Define Technical Scope**: Token-based authorization and user identity.
  3. **Threat Intelligence**: Quantum risk to token and key security.
  4. **Vulnerability Analysis**: Weaknesses in token structure and authentication.
  5. **Threat Modeling**: Focus on assets (tokens) and access points.
  6. **Risk Analysis & Evaluation**: Measure the risk of token interception.
  7. **Security Controls**: Transition to quantum-safe token algorithms.

**DNSSEC**:

* 1. **Define Objectives**: Maintain DNS integrity and authenticity.
  2. **Define Technical Scope**: Signature verification and key management.
  3. **Threat Intelligence**: Quantum risk to DNSSEC’s cryptographic signatures.
  4. **Vulnerability Analysis**: Assess key compromise risks.
  5. **Threat Modeling**: Identify DNS records as assets and query responses as potential attack vectors.
  6. **Risk Analysis & Evaluation**: Assess DNS compromise impacts.
  7. **Security Controls**: Implement quantum-safe signature algorithms.

These frameworks provide a structured approach for implementing and enhancing each protocol's security, anticipating both current and quantum-specific threats.