

Design for E2E Secure Chat Application

Security is not an after thought and it starts at Design level!

Asset(s)	<ol style="list-style-type: none">1. Database2. Messages3. Application Software4. User verification link sent while registration
Stakeholder(s)	<ol style="list-style-type: none">1. Developers2. Users
Adversary model(s)	<ol style="list-style-type: none">1. Eavesdropping adversary2. Compromise of database3. Compromise of exchange of keys
Attack Surface(s)	<ol style="list-style-type: none">1. User account details2. Database3. Configuration4. Executables5. DLL's6. Email/SMS Service7. Server8. HTTPS Protocol9. JWT