smartopia@grupo1: ~$

Análise de segurança do projeto

Grupo 1 - SmarTopia

smartopia@grupo1: ~$ cat man-in-the-middle

Man In the Middle

- **O que é:** Este tipo de ataque ocorre quando a comunicação entre duas partes é interceptada por um terceiro. Neste contexto, o invasor pode consumir o conteúdo em trânsito, modificá-lo e eventualmente se passar por uma das partes envolvidas e obtendo acesso não autorizado à informações sensíveis.

- **Como pode ocorrer no projeto:** No contexto específico de MQTT, esse ataque pode ocorrer na fase de handshake, onde o cliente e o broker estão estabelecendo a conexão ou durante a troca de mensagens.

- **Mitigação:** Uso de criptografia TLS/SSL, autenticação mútua e uso de firewalls.

smartopia@grupo1: ~$ clear && cat nosql-injection

NoSQL Injection

- **O que é:** Ocorre quando um invasor explora vulnerabilidades de segurança no sistema de banco de dados não relacional para manipular consultas ou comandos de forma maliciosa. Assim como em ataques de SQL Injection em bancos de dados relacionais, os ataques de NoSQL Injection visam explorar a falta de validação ou sanitização de entradas de dados para executar operações não autorizadas no banco de dados.

- **Como pode ocorrer no projeto:** Apesar de existir uma forma muito restrita de inserir os dados no MongoDB, utilizando drivers próprios que reforçam a segurança, payloads maliciosos podem ser injetados no banco de forma a comprometer a qualidade dos dados e consequentemente das informações.

- **Mitigação:** Práticas de segurança, como validação de entrada de dados, uso de parâmetros seguros em consultas e controle de acesso adequado ao banco de dados MongoDB.

smartopia@grupo1: ~$ clear && cat DDoS

Distributed Denial of Service (DDoS)

- **O que é:** Utilização de uma botnet (Rede de bots controlados por um atacante) para criar um fluxo excessivo de requisições maliciosas que paralisa um serviço, tornando-o inacessível para usuários legítimos .

- **Como pode ocorrer no projeto:** Um grande número de mensagens e solicitações de conexão podem sobrecarregar o broker. Sensores e dispositivos IoT podem ser suscetíveis a malwares de forma a serem configurados para enviar mensagens e consumir rapidamente os recursos do broker.

- **Mitigação:** Autenticação e autorização nos servidores MQTT, implementação de firewalls e sistemas de detecção de intrusão, atualização de firmware dos dispositivos IoT.

smartopia@grupo1: ~$ clear && cat brute-force-attack

Brute Force Attack

- **O que é:** O invasor tenta todas as possíveis combinações de caracteres para descobrir senhas, credenciais e chaves privadas.

- **Como pode ocorrer no projeto:** Para utilizar os serviços nos clusters em núvem (HIVEMQ, MongoDB e Kafka), deve-se realizar autenticação para acessá-los. Um ataque de Brute Force poderia mirar em descobrir essas credenciais a fim de desabilitar recursos e prejudicar a performance da solução.

- **Mitigação:** Uso de algoritmos de criptografia robustos, geração de chaves longas e aleatórias, evitar engenharia social.

Impacto x probabilidade	Riscos com consequências pouco significativas 1	Risco com consequências reversíveis a curto e médio prazo com custo pouco significativo 2	Risco com consequências reversíveis a curto e médio prazo com custos baixos 3	Riscos possuem consequências reversíveis a curto e médio prazo com custos altos 4	Riscos possuem consequências irreversíveis ou com custos inviáveis 5
Não é provável que aconteça 1 - 10% 1					
Pode ser que ocorra uma vez dentro de 1 ano 11 - 30% 2					
Pode ser que ocorra mais de uma vez dentro de 1 ano 31 - 50% 3		Brute Force Attack 6		NoSQL Injection 12	
Pode ser que ocorra mensalmente 51 - 70% 4		Man In The Middle 8	Distributed Denial of Service 12		
Pode ser que ocorra semanalmente 71 - 90% 5					

smartopia@grupo1: ~$ clear && cat conclusoes

Conclusões

Devido à natureza não sensível e impessoal dos dados do projeto (coleta de dados do ambiente) e sua disponibilidade pública, os impactos não são extremamente prejudiciais e podem ser contornados ativamente com poucos recursos.

Porém, ataques que visam a disponibilidade do sistema e sua integridade (funcionamento dos serviços em nuvem e qualidade dos dados) seriam mais impactantes e devem ser evitados. Nesse contexto, os esforços para implementação das mitigações apresentadas anteriormente seriam mais urgentes.