Atualmente, existem vários Sistemas Operacionais para diversos tipos de utilidades, existem aqueles que têm como foco o usuário final, como é o caso do Windows, também existem outros que são baseados em segurança, como os baseados em Unix.

2. Questões de projetos do Sistema Operacional: LynxOS

2.1. Segurança

Esse sistema demonstra várias APIs para melhorar o controle dos processadores, como também uma ampla variedade de ferramentas para desenvolvedores. Uma dessas ferramentas, é um suporte para vários sistemas de E/S, também há uma tecnologia nativa do S.O que permite acesso a recursos de segurança de última geração, além disso, podendo contar com uma série de recursos que um Sistema Operacional de tempo real oferece. Garantindo que E/S, mesmo que previsível, seja garantida no resultado final do escalonamento exclusivo e também um kernel otimizado (GARCIA,2017).

Em um Sistema Operacional de tempo real, existe um compromisso de promover a proteção do sistema em pontos problemáticos. Um ponto em comum para esse tipo de sistema operacional são as interrupções (ACCELERATED TECHNOLOGY, 1999). Essas representam mecanismos responsáveis por modificar o caminho de execução do processador (SILVA, 2011) e transferem o controle para a rotina de serviço de interrupção (RSI) (ACCELERATED TECHNOLOGY, 1999).

Os problemas surgem justamente nos acessos de serviços no sistema por RSIs. A forma de tratar esses casos é protegendo as estruturas de dados acessadas simultaneamente por uma chamada de serviço e uma RSI. Utilizando-se a solução mais simples, encontra-se também um impasse, onde o sistema de tempo real não cumpre a tarefa de responder as interrupções rapidamente, por ter como resposta para o problema, o bloqueio de interrupções durante uma chamada de serviço (ACCELERATED TECHNOLOGY, 1999).

Com isso, a solução disponibilizada, foi a divisão de RSI em níveis: baixo e alto. No nível baixo se utiliza apenas alguns recursos do S.O., salvando o contexto antes de chamar a RSI e na sequência, ao finalizar a rotina, restaurando o contexto. Já no nível alto, as RSIs são criadas e excluídas dinamicamente e possuem espaço de memória apropriado para controle, permitindo o bloqueio ao tentar acessar uma estrutura de dados que já está sendo acessada (ACCELERATED TECHNOLOGY, 1999).

O Nucleos RTOS trata, também no quesito proteção, considerando a confiabilidade que o sistema deve apresentar. Assim, deve-se disponibilizar armazenamento e transmissão de dados de forma segura. Para empregar autenticidade, integridade e confidencialidade, o sistema utiliza tecnologias disponíveis e seus respectivos recursos (MENTOR GRAPHICS CORPORATION, 2018).

A (MENTOR GRAPHICS CORPORATION, 2018) apresenta uma lista dos recursos utilizados para garantir a segurança proposta. São eles:

• Algoritmos de criptografia simétrica e assimétrica;

• Algoritmos de hashing de dados;

• Protocolos de criptografia;

• Suporte à criptografia de chave pública;

• Opções de verificação por pares.

Referência

GARCIA, Lukas W. Real-Time Operating Systems Case Study. 2017.