DNSSEC

Ienne, flavio

- Torna o processo de resolução de nomes mais seguro;
- Extensão do protocolo DNS para adicionar mecanismos de segurança;
- Permite que se possa verificar as informações recebidas, invés de “confiar” em sua validade
- Usa criptografia assimétrica para verificar

autenticidade e integridade dos dados;

Vulnerabilidades do DNS

- Inexistência de garantia de autenticidade de origem.
- Inexistência de garantia de integridade dos dados.
- Ausência de segurança do canal de comunicação.
- Impossibilidade de efetuar uma negação de origem autenticada, isto é, não há maneira de se verificar a inexistência de um nome.

DNSSEC

- Autenticidade de origem: Os dados que foram recebidos em retorno a uma consulta devem originar-se apenas de dentro da zona que foi solicitada;
- Integridade dos dados :O retorno de uma consulta deve conter dados idênticos aos enviados pelo servidor de nomes;

- Negação de autenticidade de existência
  Caso o retorno de uma consulta seja de que o domínio não exista, essa informação deve ser assegurada;

- uma chave privada assina com a zona raiz. O resolver fica com posse de uma chave publica que verifica a informação. Cada zona garante a autenticidade de sua resposta usando uma assinatura digital e também oferece uma maneira de assegurar que as assinaturas das zonas de nıvel abaixo do seu podem ser seguras.

No Brasil

- O poder Judiciário mais alguns órgãos públicos, juntamente com alguns bancos vem aderindo a essa nova tecnologia.
- Esta sendo implantado peloRegistro.br