Encrypted Client Hello (ECH) for Enterprises

• This document is not a critique of ECH, it tries to look beyond
• Enterprises are facing a set of requirements and constraints
  • Compliancy, Risks, Threat landscape, etc.
• This leads to
  • An evolution of the defense and operational security (from X.800 to ZT, SSE, MESH, etc.)
  • The need for network security controls and selective decrypt (e.g. to perform DLP)
• By removing access to the SNI, ECH pushes security to the endpoints
  • Unfortunately, this paper shows neither device nor browser can be trusted (MITB)
  • Worse, beyond the SNI, the only way to protect the user is to read the full page
  • The browser cannot be judge and party
• Or ECH is pushing the security to the client facing server?
  • This would make the client facing server a middlebox?
  • Is it an untapped opportunity?
Questions and Call for Action

• The Client Facing Server vs Backend Server relationship is unclear
  • can it be really left to ‘just’ implementation?
  • Is the Client Facing Server a ‘protocol’ based way to do middleboxes?

• If the ECH constituencies cannot be judge and parties how to integrate a 3rd party security component?

• Is there a form of recognition/acknowledgment of enterprises operational security problem?
  • An answer yes or no will lead to two different developments

• PROPOSAL for an adhoc session on 26th of July at 1:30pm EST / 7:30 CEST
  • Contact Arnaud.Taddei@broadcom.com