# Attacking the IPsec Standards When Applied to IPv6 in Confidentiality-only ESP Tunnel Mode

Dongxiang Fang, Peifeng Zeng, Weiqin Yang

*College of Computer Science and Technology, Donghua University, Songjiang, Shanghai 201620, China*

***fdx321@126.com, zengpf@yahoo.com, july0810@163.com***

*Abstract*—**Attacks which can break RFC-compliant IPsec implementation built on IPv6 in confidentiality-only ESP tunnel mode are proposed. The attacks combine the thought of IV attack, oracle attack and spoof attack to decrypt a encrypted IPv6 datagram. The attacks here are more efficient than the attacks presented by Paterson and Degabriele because no checksum issue has to be handled. The paper shows that using IPsec with confidentiality-only ESP configuration is insecure to convince users to select it carefully.**

*(Pt9)Keyword*—**IPsec, IPv6, ESP, confidentiality-only, Security**

**Dongxiang Fang** received a B.E. degree in software engineering from Donghua University in 2012. He is currently studying in Donghua University for M.S. degree in computer science and technology. His research interests are in areas of network protocols, image processing and pattern recognition.

**Peifeng Zeng** received the B.E. and M.E. degrees from Southeast University in 1984 and 1990, respectively. He received the PhD degree from Nagoya University in 2002. He is currently a professor in College of Computer Science and Technology, Donghua University. Hi research areas are embedded systems, image processing and pattern recognition. Mr. Zeng is a member of the IEEE and the ACM.

**Weiqin Yang** received her B.E degree in Network Engineering from DongHua University, China, in 2013. She has been studied in DongHua University for her M.E degree in Computer Science and Technology since 2013. Her research interests are in areas of image recognition and tracking.