โลกกำลังก้าวสู่อินเทอร์เน็ตที่ปลอดภัยกว่าเดิม

นำเสนอเมื่อ : 10 ต.ค. 2551

โลกอินเทอร์เน็ตถูกสร้างขึ้นมาบนพื้นฐานของความเชื่อใจกันนับแต่วันแรก เราคงจำกันได้กับวันที่เราเคย finger ว่าใครออนไลน์บนเครื่องไหนกันบ้าง เพราะยุคแรกของอินเทอร์เน็ตนั้นมันเป็นช่องทางเชื่อมต่อระหว่างนักวิจัยเป็นหลัก

แต่ในยุคนี้ที่อินเทอร์เน็ตนั้นเต็มไปด้วยอันตราย ความเชื่อใจแบบเดียวกันนี้ แม้จะลดลงอย่างมากในช่วงหลายปีมานี้ แต่เรายังคงล็อกอินเว็บด้วยการเชื่อมต่อแบบไม่เข้ารหัส ไวร์เลสแลนของเราส่วนมากมีการป้องกันเพียงเล็กน้อย หรือไม่มีการป้องกันใดๆ เลย ปัญหาหลักในเรื่องนี้คงเป็นเรื่องของความยุ่งยากในการติดตั้ง แต่ความเป็นจริงอีกอย่างหนึ่งคือการเพิ่มความปลอดภัยให้อินเทอร์เน็ตนั้นมีค่าใช้จ่ายที่แพงมาก การเข้ารหัสแบบ **TLS** ให้กับการเชื่อมต่อทั้งหมด หมายถึงการคำนวณปริมาณมากมายให้กับผู้ใช้ทุกๆ คนโดยที่เซิร์ฟเวอร์ไม่สามารถแคชผลการคำนวณไว้ใช้งานได้ แต่โลกกำลังเปลี่ยนแปลงไปด้วยสองเทคโนโลยีหลัก

การทำงานแบบมัลติเธรด ที่กระจายงานไปยังหลายๆ **ซีพียู**ได้ เมื่อผู้ใช้เพิ่มขึ้น การเพิ่มจำนวนคอร์ของซีพียูช่วยให้เราสามารถรองรับผู้ใช้ที่เพิ่มขึ้นเหล่านั้นได้

Multi-Core เช่น **Core 2** เป็นการใส่ซีพียูจำนวนมากกว่าหนึ่งชุดเข้าไปในแพคเกจเดียวกัน ทั้งสองคอร์มักจะสามารถสื่อสารถึงกันได้เร็วเป็นพิเศษทำให้แชร์ข้อมูลกันได้ง่าย

SMT เป็นการแยกร่างซีพียูคอร์เดี่ยวให้ทำงานเสมือนว่ามีสองคอร์ไป ผลที่ได้อาจทำให้หลายๆ คนแปลกใจคือหากเราสามารถแยกงานออกเป็นสองเธรด แล้วทำงานบนซีพียูแบบ **SMT** แล้ว ผลลัพธ์จะเร็วขึ้น 14-200% เลยทีเดียว

การใช้ซีพียูแบบเฉพาะทาง ลองนึกถึงการ์ดกราฟิกที่ทำหน้าที่คำนวณข้อมูลสามมิติโดยเฉพาะ ทำให้มันทำงานได้เร็วอย่างไม่น่าเชื่อ การเข้ารหัสก็สามารถใช้ชิปแบบเฉพาะได้เช่นกัน แต่ใน Core Microarchitecture ได้มีการใส่คำสั่งหลายคำสั่งเพื่อเพิ่มความเร็วการเข้ารหัสมาอยู่แล้ว คือ

ชุดคำสั่ง **AES** ได้แก่ **AESENC, AESENCLAST, AESDEC, และ AESDECLAST** ชุดคำสั่งเหล่านี้สามารถเร่งความเร็วการเข้ารหัสในแบบ AES ให้เร็วกว่าการใช้คำสั่ง x86 ตามปรกติได้ประมาณสามถึงสี่เท่าตัว

ชุดคำสั่งการคูณแบบเป็นชุด ได้แก่ **PCLMULQDQ** ซึ่งเป็นคำสั่งคูณเลข **64 บิต**ทีละสี่ชุดพร้อมๆ กัน การคูณจำนวนมากๆ นั้นเป็นเรื่องปรกติมากในการเข้ารหัสแทบทุกอัลกอลิธึ่ม

ดังนั้นคำสั่งแบบนี้จึงสามารถช่วยเพิ่มความเร็วการเข้ารหัสได้แทบทุกรูปแบบ

การเปลี่ยนแปลงเช่นนี้ยังต้องการการปรับปรุงจากโลกซอฟต์แวร์อีกมากให้สามารถทำงานโดยใช้ทรัพยากรในซีพียูได้อย่างเต็มที นับแต่การคอมไพล์ใหม่เพื่อให้ซอฟต์แวร์ใช้คำสั่งใหม่ๆ ได้ หรือการออปติไมซ์ในด้วยมือตลอดจนการเปลี่ยนแปลงสถาปัตยกรรมซอฟต์แวร์ใหม่ทั้งหมด

ข้อมูลจาก **สนุก.คอม**