อันตราย 5 ประการของระบบเครือข่าย (Networks) ที่ไม่มีการรักษาเวลาที่แม่นยำพอ ปัญหาที่พบได้ทั่วไปเมื่อระบบเวลาของเครือข่ายไม่มีการมีการประสานกัน (Synchronization) อย่างพร้อมเพรียง ย่อมจะต้องเกิดปัญหาร้ายแรงที่ไม่คาดคิดขึ้นแน่นอน อย่างไรก็ตาม หนทางออกที่จะกล่าวในบทความนี้คุณจะพบว่าเป็นสิ่งที่ทำได้ง่าย โดยไม่ต้องใช้เงินมหาศาลแต่มีประสิทธิผล

บทนำ

องค์กรต่างๆ เกือบทั้งหมดในทุกวันนี้ต้องพึ่งพาเครือข่ายของคอมพิวเตอร์ ตั้งแต่ระบบ LAN ขึ้นไป ซึ่งทั้งหมดจะต้องพึ่งพาระบบนาฬิกาของคอมพิวเตอร์ แล้วจะเกิดอะไรขึ้นเมื่อนาฬิกาของระบบคอมพิวเตอร์เหล่านี้ แสดงเวลาที่แตกต่างกันหรือ แสดงเวลาที่ผิดพลาด แล้วถ้าคิดต่อว่าจะเกิดอะไรขึ้นจากกระบวนการที่ทำงานอยู่บนเครือข่ายเหล่านี้ จนถึงอะไรจะเกิดขึ้นตามมากับองค์กรที่ใช้เครือข่ายเหล่านี้

ระเบิดเวลากำลังเดินอยู่ท่ามกลางหัวใจของโครงสร้างไอทีเกือบทั้งหมด โครงสร้างซึ่งองค์กรต่างๆ ต้องอาศัยพึ่งพาในการผลิตสินค้า การซื้อขายสินค้า การเตรียมรายงานทางการเงิน และการสื่อสารทั้งภายในและภายนอกองค์กร หรือทุกสิ่งทุกอย่างในองค์กรยุคไอทีที่จะต้องกระทำ เมื่อระบบฐานเวลาของเครือข่าย (Network) เหล่านี้ ปราศจากการประสาน(Synchronization) ระหว่างเครื่องด้วยกัน หรือกับเวลามาตรฐานที่ถูกต้อง สิ่งเลวร้ายย่อมจะเกิดขึ้นมา ส่งผลให้กระบวนการต่างๆ จะความล้มเหลว มีการสูญเสียข้อมูล ระบบความปลอดภัยหละหลวม และองค์กรสูญเสียความน่าเชื่อถือต่อลูกค้าและพันธมิตรทางธุรกิจ ทำไมระเบิดเวลาเหล่านี้ถึงถูกปล่อยให้เกิดขึ้น เป็นเพราะว่าผู้คนทั่วไปทึกทักด้วยความเข้าใจผิดว่า ระบบนาฬิกาของคอมพิวเตอร์มีความแม่นยำในตัวมันเอง นั้นเป็นสิ่งที่ไม่ความเข้าใจอย่างถ่องแท้ถึงกระบวนการ และขั้นตอนที่ทำให้คอมพิวเตอร์เหล่านี้จำเป็นต้องความเกี่ยวข้องสัมพันธ์กัน หากเวลาในคอมพิวเตอร์เหล่านี้ไม่สัมพันธ์อย่างถูกต้อง ท้ายที่สุดพวกเขาไม่ได้ตระหนักเลยว่าทางออกของปัญหาในการประสานเวลาเครือข่าย (Synchronization Network) เป็นเรื่องที่ไม่ได้ใช้เงินเยอะ และง่ายต่อการนำมาใช้ ทางออกนี้เรียกว่า Time Server ซึ่งมีราคาอยู่ในหลักแสน และสามารถให้การรองรับเครือข่ายที่ประกอบด้วยคอมพิวเตอร์นับพัน และอุปกรณ์แบบนี้ทำงานโดยที่เราแทบจะไม่ต้องใส่ใจ ดังนั้นจึงเป็นสิ่งที่ไม่มีเหตุผลโดยสิ้นเชิง ที่เหตุใดจึงปล่อยให้อันตรายต่างๆที่จะได้กล่าวดังต่อไปในเอกสารนี้เกิดขึ้นโดยที่ไม่มีการใส่ใจ

อันตราย 5 อย่างของการปล่อยให้คอมพิวเตอร์ในเครือข่ายทำงานโดยที่ไม่มีการประสานเวลา (Synchronization) แบ่งออกได้เป็น 5 หมวดใหญ่ๆ

1.กลไกการทำงานล้มเหลว

กระบวนการอัตโนมัติ อย่างเช่น การสำรองข้อมูลหรือกระบวนการคำสั่งซื้อจะไม่เกิดขึ้นหรือจะล้มเหลว ที่เป็นเช่นนี้เพราะกระบวนการที่จะกระตุ้นให้เกิดการทำงาน ณ เวลาที่กำหนดไม่เกิดขึ้น หรืออาจเป็นเพราะภาระที่กำหนดที่คาดหวังว่าจะเกิดขึ้นในคอมพิวเตอร์เครื่องอื่นๆ ไม่สามารถถูกกระทำได้ในลำดับที่ถูกต้อง

2. การสูญหายของข้อมูล

ซึ่งเกิดขึ้นได้เพราะซอฟแวร์ระบบยึด อย่างเช่น ระบบข้อมูล (Directory) ทำการบันทึกแฟ้มที่มีเวอร์ชั่นที่เก่าเกินไปเป็นเวอร์ชั่นล่าสุด

3. ระบบรักษาความปลอดภัยเกิดช่องโหว่

ซึ่งเกิดขึ้นได้ทั้งโดยตรงและโดยอ้อม สำหรับระบบที่ไม่มีการรักษาความแม่นยำของเวลาเป็นของระบบเองโดยตรง ตัวอย่างเช่น เครือข่ายเกือบทั้งหมดจะทำการตั้งเวลาโดยใช้โพรโตคอลประสานเวลาชื่อ NTP หรือ Network Time Protocol ซึ่งจะทำการเปิด Firewall ให้กับ Hacker สามารถเจาะทะลุเข้ามาในเครือข่ายได้ นอกจากนี้การแก้ไขยังมีปัญหาเกิดขึ้นตามมาเพราะผู้ดูแลระบบไม่สามารถติดตามร่องรอยของ Hacker ได้ เนื่องจาก log file ไม่มีการประทับเวลาที่แม่นยำพอ นอกจากนี้ Application เกี่ยวกับความปลอดภัย นั้นเป็นลักษณะ Batch Reader ซึ่งถูกออกแบบมาให้ทำการปกป้องทรัพย์สินของบริษัทจะหยุดทำงานด้วย

4. ความรับผิดชอบทางกฎหมาย

เมื่อมีข้อขัดแย้งในทางการค้า ไม่มีทางใดเลยที่จะทำการพิสูจน์ได้ว่าเกิดธุรกรรมขึ้นตามที่กล่าวอ้าง หรือลายเซ็นดิจิตอลบนสัญญาเป็นของแท้

5. การขาดความน่าเชื่อถือ

อันตรายที่กล่าวมาทั้งหมดหมายถึงการสูญเสียธุรกิจ เช่นเดียวกันเป็นการแสดงให้เห็นถึงการขาดความสามารถในการแข่งขันในธุรกิจ ความน่าเชื่อถือทางธุรกิจเป็นสิ่งที่ต้องใช้เวลา

เราจะกล่าวถึงอันตรายทั้งหมดเหล่านี้โดยละเอียด

ข้อแรก ความล้มเหลวของกระบวนการทำงาน ความล้มเหลวนี้ครอบคลุมถึงกิจกรรมที่หลากหลายซึ่งเกี่ยวข้องกับทุกส่วนของบริษัท

ปัญหาแบ่งออกได้เป็น 3 กลุ่ม คือ ระบบงานอัตโนมัติ ภาระ Network Consolidated และ Application ที่เกี่ยวข้องกัน

1. ระบบงานอัตโนมัติ เช่นการสำรองข้อมูล ซึ่งมักจะทำงานในเวลากลางคืนจะเป็นเหตุการณ์ที่ประกอบขึ้นจากหลายขั้นตอน ซึ่งแต่ละขั้นตอนจะเกิดขึ้นตามเวลาที่กำหนด หากมีเหตุการณ์ใดเหตุการณ์หนึ่งถูกกระตุ้นให้เกิดขึ้นนอกกระบวนการหรือนอกลำดับที่ตั้งไว้ อาจจะทำให้กระบวนการทั้งหมดล้มเหลว ยิ่งไปกว่านั้น เนื่องจากภาระหน้าที่เหล่านี้มักจะเกิดขึ้นนอกช่วงเวลาทำงานปกติ จึงเป็นไปได้อย่างสูงว่าความล้มเหลวที่เกิดขึ้นจะไม่ถูกค้นพบ หรือถูกแก้ไขจนกระทั้งในวันทำงานต่อมา

2. กระบวนการงานที่เกี่ยวข้องกับ Network บางอย่างอาจจะทำการประหยัดทรัพยากรของระบบ โดยการใช้เครื่องเพียงเครื่องเดียวในการกระทำงานบริการร่วมกันของคอมพิวเตอร์เครื่องอื่นๆ แทนที่จะให้เครื่องคอมพิวเตอร์เครื่องอื่นๆ ต่างกระทำภาระนั้นของตนเอง กระบวนการอื่นๆ เช่น การประสานเวลา จะถูกกระทำโดยเครื่องรวมไม่ทางใดก็ทางหนึ่ง กระบวนการจะแสดงความล้มเหลวได้เพียงจุดเดียว บริการ Directory เช่น Windows NT Directory, Novell Directory Service และ Group ware เช่น Microsoft Exchange หรือ Lotus Note จะใช้ Time Source ร่วมกันในการกำหนดคำสั่งที่เหตุการณ์จะเกิดขึ้น หาก Server ซึ่งกระทำตนเป็น Time Source ร่วม ไม่มีการประสาน (Synchronize) กับนาฬิกาของ Work Station อื่นๆ รวมถึง Server ซึ่งทำหน้าที่ควบคุมปฏิบัติการหรือคำร้องขอใดๆ จากผู้ใช้หรือ จาก Application ที่อยู่บนเครื่องเหล่านี้อาจจะไม่ได้รับการยอมรับว่าถูกต้อง

สถานการณ์คล้ายคลึงกันนี้เกิดขึ้นได้เช่นเดียวกันกับ Distributed Commuting Middle Ware เช่น IBM PCE Middle Ware เป็นการทำการเชื่อมต่อกระบวนการที่รันอยู่บนเครื่องหลายเครื่อง ให้เป็นเหมือนกับว่าเป็น Application เดียวกัน ตัวอย่างเช่นการจัดการคำสั่งซื้อ การออกบิลที่จุดขาย หรือการควบคุมสินค้าคงคลัง ต่างก็ทำงานร่วมกันทั้งหมด ในกรณีของ PCE หากนาฬิกาของเครื่องในกระบวนการต่างๆ แตกต่างกันมากกว่า 5 นาที เมื่อเทียบกัน DCE Distributed Time Server กระบวนการเหล่านั้นจะล้มเหลว ซึ่งอาจจะรวมถึงระบบออกบิลที่จุดขาย หรือส่วนหนึ่งส่วนใดของโครงสร้าง ที่เกี่ยวข้องกับกับระบบคอมพิวเตอร์ที่ต้องมีเวลาที่แม่นยำ เป็นต้นว่า การควบคุมการผลิต การตั้งเวลาของระบบสื่อสารเครือข่าย การดูแลรักษาระบบของคอมพิวเตอร์ การโอนเงิน หรือซื้อเงิน การประทับเวลาที่แฟ้มฐานข้อมูล เช่น NFX Unix เป็นต้น

การตรวจสอบความล้มเหลว

การตรวจสอบความล้มเหลวผ่าน SNMP Event Trap การประทับเวลาสำหรับการบันทึก เวลาจากโทรศัพท์หรือวิทยุในงานส่วนบุคคล การบันทึกเวลาพนักงาน การจัดเวลา Pelage time sys การตามแกะรอยผู้บุกรุก การรักษาความปลอดภัยที่ขึ้นอยู่กับเวลา เช่น Turbinate Ostentation การประทับ Package Time Right Application ต่างๆ ไม่จำเป็นต้องเป็นส่วนหนึ่งของ Distributor Commuting Evaluation เพื่อให้สามารถขึ้นต่อกัน จริงๆ แล้วคู่ค้าทางธุรกิจอาจจะไม่ต้องการถูกล็อกเพื่อทำการ Middle Ware lager เพียงเพื่อพวกเขาจะได้สามารถทำธุรกิจได้ และพวกเขาไม่จำเป็นต้องทำเช่นนั้น มีหลายวิธีการที่จะทำให้ Application สามารถสื่อสารซึ่งกันและกัน เป็นต้นว่า โดยการใช้ EPD หรือ XML ไม่ว่าจะเป็นวิธีการใด ความต้องการในการ Synchronize ยังคงสูงอยู่เป็นต้นว่า เมื่อผู้ผลิตชิ้นส่วน ทำการส่ง stock สินค้าให้กับผู้ผลิตรถยนต์ แบบ just in time การทำธุระกรรม แต่ละครั้ง พร้อมกับส่วนประกอบ

หลากหลาย จะถูกประทับเวลา ซึ่งโดยทั่วไปจะยอมรับความผิดพลาดได้ภายในไม่เกิน 1 วินาที หากรายการวัสดุของผู้ขายหรือราคาไม่ได้รับการรับโดยลูกค้าซึ่งกำลังรอภายในเวลาที่กำหนด Application ของลูกค้า อาจจะเปลี่ยนไปทำธุรกรรมขั้นตอนอื่น ซึ่งเป็นเหตุการณ์ที่เกิดขึ้นได้ หากเวลาที่ประทับผิดพลาดแสดงให้เห็นถึงว่า ข้อมูลที่ถูกส่งออกไปก่อนที่มันจะถูกร้องขอ หรือไปถึงก่อนที่ที่มันจะถูกส่งออกไป ตัวอย่างอื่นๆ เช่น E-mail ถ้าโปรแกรม E-mail ของผู้ใช้ถูกตั้งให้แสดงข้อความเรียงลำดับตามเวลาที่ส่งข้อความที่มาพร้อมกับเวลาที่ผิดพลาด อาจจะถูกมองข้าม หรือเรียงลำดับผิดพลาด

การสูญเสียข้อมูล

การสูญเสียข้อมูลเกิดขึ้นได้กับกระบวนการทำงานทางเดียว การสูญเสียข้อมูลไม่เหมือนการล้มเหลวอื่นๆคือมันอาจไม่ได้ถูกตรวจพบเป็นเวลานาน ซึ่งสร้างความเสียหายมากยิ่งขึ้น เพราะผู้คนหรือ Application จะพึ่งพาข้อมูลที่เชื่อว่าถูกต้อง แต่ที่จริงมันไม่ถูกต้อง ตัวอย่างที่สำคัญเช่น ระบบทรัพยากรเครือข่ายซึ่งทำการเก็บรักษาประวัติของวันทีและเวลา ที่แฟ้มได้ถูกสร้างขึ้น ถูกแก้ไขล่าสุด ถูกเข้าถึงล่าสุด และถูก uptight ล่าสุด ถ้ามีเครื่องหนึ่งเครื่องในระบบ ส่งแฟ้มซึ่งประทับด้วยเวลาเร็วกว่าของแฟ้มที่เก็บรักษาใน Server กลาง Server นั้นอาจจะถือว่าไฟล์นั้นเป็นไฟล์เก่า และละเลยการเปลี่ยนแปลงใดๆ ที่เกิดขึ้น อีกตัวอย่างหนึ่งได้แก่ การพัฒนา Software ที่ต้องประทับเวลาระบุส่วนประกอบของ Software ที่เขียนมาจากเครื่องต่างๆ และเป็นไปได้ว่า Version ที่ถูกแสดงที่ Control File System จะเป็นไปตามลำดับแทนที่จะเป็นตามเวลาที่มันถูกเขียนขึ้น นั้นหมายถึงว่า Software เวอร์ชั่นล่าสุดจริงแต่ส่วนประกอบไม่ใช่เวอร์ชั่นล่าสุด ส่งผลให้การทำงานของ Software ผิดพลาดหรือไม่ทำงานเลย โปรแกรมเมอร์ต้องเสียเวลาเป็นอาทิตย์ในการมองหาข้อผิดพลาด ทั้งทีจริงปัญหาไม่ได้เกี่ยวข้องกับรหัสคำสั่งเลย

ช่องโหว่ของระบบรักษาความปลอดภัย

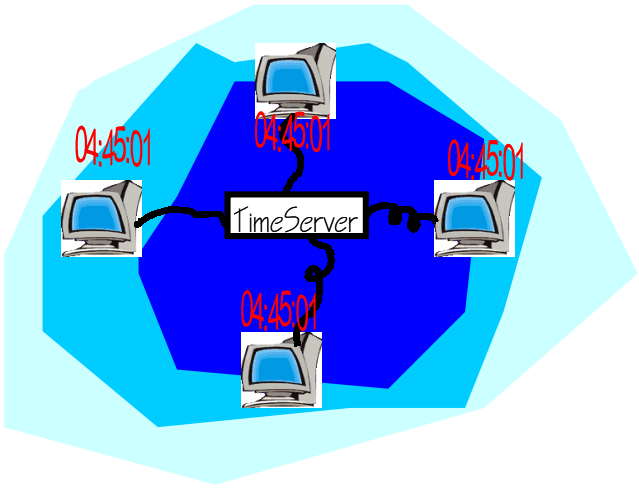
ช่องโหว่ที่เกิดขึ้นจากที่องค์กรต่างๆ ทำการรักษาเวลาเครือข่าย มีผลกระทบโดยตรงต่อความปลอดภัยของทั้งระบบ IT ในองค์กรนั้นด้วยเหตุผล 2 ประการ

ประการแรก กลไกการรักษาเวลาที่เคยใช้ ถูก Hacker ใช้ประโยชน์ในการเข้าถึงเครือข่าย

ประการที่สอง การประทับเวลาใช้เป็นข้อมูลในการแกะรอย Hacker ในระบบไม่แม่นยำ และเป็นอุปสรรคต่อการป้องกันการจู่โจมครั้งต่อไป ส่วนจุดอ่อนที่เกิดจากการประสานเวลาคือ การสื่อสารระหว่างเครือข่ายคอมพิวเตอร์เป็นการใช้โปรโตคอลสื่อสารแบบ TCP/IP ที่เรียกว่า NTP (Network Time Protocol) ถ้าประสานเวลาออกนอก Firewall ไม่มีทางแน่ใจเลยได้ว่ามาจากแหล่งที่เชื่อถือหรือถูกต้องหรือเปล่า และความเสี่ยงสูงมากที่จะถูกปลอมแปลงจากผู้ไม่ประสงค์ดี โดยปกติ NTP จะใช้งาน Port หมายเลข 123 ตลอด และแน่นอน Hacker ทุกคนรู้ดี จากนั้นคงเดาได้อะไรจะเกิดขึ้นกับเครือข่ายบ้าง ท้ายที่สุดยังมีเรื่องของประสิทธิภาพของระบบป้องกันความปลอดภัยในเครือข่ายเองที่จะต้องพิจารณา รวมถึง Firewall , Access Card Reader และการตรวจสอบความถูกต้องของลายเซ็นอิเล็กทรอนิกส์ (Digital Certificate) ซึ่งเรื่องเหล่านี้เกิดปัญหาได้ถ้าเวลาในเครือข่ายไม่แม่นยำเพียงพอ เช่น ระบบการตรวจสอบความถูกต้องของ Digital Certificate ซึ่งถูกใช้ในการตรวจเช็ค Certificate ที่ใช้ในการอนุมัติการจ่ายเงิน การเซ็นสัญญารวมถึงธุรกิจอื่นๆ ที่ต้องการ การตรวจสอบในการตรวจสอบความปลอดภัยเบื้องต้น Certificate จะถูกส่งออกพร้อมกับช่วงระยะเวลาหนึ่ง ซึ่งจะต้องถูกทำซ้ำเป็นระยะๆ ถ้าเครือข่ายไม่ประสานเวลาได้อย่างถูกต้อง Certificate ที่หมดอายุไปแล้ว อาจจะสามารถใช้ได้อยู่ซึ่งจะเป็นปัญหาต่อความปลอดภัย ปัญหาคล้ายคลึงกันเกิดขึ้นเช่นเดียวกับระบบ Fire wall ซึ่งอาจจะถูกเปิดชั่วคราวในระหว่างวัน เป็นต้นว่าในระหว่างกระบวนการ maintenance หรือการ upload file จาก Server ที่อยู่ห่างไกล ถ้าเวลาของระบบไม่ได้ถูกต้อง Firewall เหล่านี้อาจจะถูกเปิดโดยไม่ได้ตั้งใจ ตัวอย่างในทางกลับกันคือ Access Card Reader กรณีที่มีการไม่มีการประสาน (sync) ของเวลาเกิดขึ้นอาจจะทำให้เกิดความล้มเหลวในการแยกแยะ Card ที่ถูกต้อง ซึ่งเกิดขึ้นได้เพราะ Card และตัวอ่านใช้เวลาปัจจุบันในการกำหนดรหัส Entry ถ้านาฬิกาไม่มีการประสานกัน ทั้ง Code และ Card จะไม่ทำงาน

ภาระทางกฎหมาย

การรักษาเวลาที่แม่นยำในเครือข่าย ไม่ใช่เป็นเพียงเรื่องทางด้านเทคนิค แต่ยังคงเป็นเรื่องทางด้านกฎหมายเช่นเดียวกัน ทั้งนี้เพราะเวลาถูกใช้เป็นพื้นฐานในการทำสัญญา ในโลกแห่งความเป็นจริงผู้คนได้รับใบเสร็จรับเงิน เซ็นสัญญา และตรวจสอบประสิทธิภาพ เอกสารเหล่านี้ลายเซ็นและธุระกรรมล้วนแต่ใช้เวลาอ้างอิงทั้งสิ้น ซึ่งทำให้เป็นข้อผูกพันธ์ทางกฎหมาย ล่าสุดทั้งสหรัฐอเมริกาและยุโรป ได้ผ่านกฎหมายให้เอกสารที่เซ็นด้วยระบบ Digital เป็นสิ่งที่ถูกต้องตามกฎหมาย เมื่อการกระทำสัญญาในโลกไซเบอร์เป็นสิ่งที่เกิดขึ้นทั่วไป ทุกฝ่ายที่ทำสัญญาออนไลน์ หรือธุระกรรมออนไลน์จะถูกเรียกให้ทำการพิสูจน์มากขึ้น ว่าสิ่งที่กล่าวอ้างว่าได้เกิดขึ้นจริงๆ และเกิดขึ้นเมื่อใด ลองพิจารณาดูธุรกิจค้าหุ้น จะพบความจริงที่ว่าสมาคมนักค้าหุ้นแห่งชาติ ซึ่งประกอบด้วยเครือข่ายสมาชิก 5,500 คน และสำนักงานสาขา 80,200 แห่ง สมาชิกทุกรายจะต้องทำการประทับเวลาสำหรับการค้าหุ้นโดยมีความถูกต้องแม่นยำภายใน 3 วินาที ยิ่งไปกว่านั้นสมาชิกจะต้องสามารถพิสูจน์ได้ว่าเวลาที่ประทับมาจาก Time Source ที่ยอมรับได้ โดยเฉพาะจาก NIST (สถาบันมาตรฐานทางมาตรวัดแห่งสหรัฐอเมริกา) ในการทำธุรกรรมอิเล็กทรอนิกส์นั้น การมีแต่แหล่งประสานเวลา (Time Source) ภายในเครือข่ายเองนั้นยังไม่เพียงพอ แต่มันจะต้องมีแหล่งประสานเวลาภายนอกที่ยอมรับได้ทั่วโลกด้วย



การสูญเสียความน่าเชื่อถือ

จากอันตรายที่ได้กล่าวมาแล้วทั้งหมด บางที่สิ่งที่อันตรายที่สุดคือการสูญเสียความน่าเชื่อถือในตลาดนี้เป็นสิ่งที่เห็นได้ชัดเจน ยิ่งกระบวนการล้มเหลวมากเท่าใด ก็ยิ่งสูญเสียข้อมูลมากเท่านั้น ยิ่งมีปัญหาความปลอดภัยเกิดขึ้นมากเท่าใด ภาระทางกฎหมายก็ยิ่งมากขึ้นเท่านั้น และจะทำให้เป็นการยากที่จะดึงดูดธุรกิจต่อธุรกิจ บริษัทจะต้องยุ่งเหยิงกับการต่อสู้ปัญหาเหล่านี้ แทนที่จะใช้เวลาไปในการเอาใจใส่ต่อธุรกิจหรือลูกค้า แต่ใช่ว่าปัญหาจะยากจนเกินแก้ไข ซึ่งการรักษาเวลาเป็นสิ่งที่ทำได้ง่ายราคาไม่แพง และมีประสิทธิภาพอย่างสูงในการที่จะหยุดยั้งปัญหาเหล่านี้ของบริษัท

ถ้าหาก Time Source ที่ว่านี้ไม่ได้อยู่ภายใน Firewall ของบริษัทซึ่งนั้นก็หมายความว่าจะมีการเปิดช่องว่างภายใน Firewall โดยเฉพาะ Port 123 เพื่ออนุญาติให้แพ็กเกจข้อมูลซึ่งบรรจุข้อมูลของเวลาผ่านออกได้ ถึงแม้ว่า Time Source จะไม่ได้อยู่ภายนอก File Wall ก็ไม่ได้หมายความว่า Port 123 จะถูกปิดโดยอัตโนมัติ เป็นเพียงแต่ว่ามันไม่จำเป็นต้องถูกใช้ ผู้บริหารระบบจึงจำเป็นที่จะต้องตรวจดูให้แน่ใจว่า Port ที่ไม่ได้ถูกใช้งานจะถูกปิดเสมอ

วิธีการที่หนึ่ง ในการอาศัยช่องว่างที่เปิดนี้คือการอัดข้อมูลกับโปรแกรม NTP อยู่ในตัวมันเองซึ่งสามารถถูกทำไว้โดยตัวแปรหลายประการทั้งยูนีกส์ และลีนุกซ์ โอเปอเรทติ่ง ซิสเตม โดยการส่งข้อมูลที่มากเกินไปใน NTP Package ผลคือการปฏิเสธให้บริการเวลาและเกิดการภาวะชะงัก (Cash)ของ Network ในตัวมันเอง

วิธีการที่สอง ในการอาศัย NTP คือการสร้าง Package ที่ไม่ได้ทำการ Clash NTP โปรแกรม หากแต่ใช้โปรแกรมนั้นในการเข้าไปควบคุมเครื่องเป้าหมายโดยอาศัยสิ่งที่ได้รับอนุญาตในโปรแกรม NTP ซึ่งโดยปกติจะเป็นระดับของ System Admin ถึงแม้ว่าองค์กรจะทำการปิดกั้นการ Access เข้าไปยัง Port 123 ยกเว้นแต่ที่ได้จาก Time Source ภายนอกแต่นั้นก็ยังคงเปิดช่องว่างสำหรับความเป็นไปได้ที่ Hacker จะทำการโจมตี Network จากจุดนั้น

ผลร้ายของการรักษาเวลาที่อ่อนแอยังมีมากขึ้นอีกนั้นคือมันได้ทำลายความสามารถในการตรวจสอบและค้นหาร่องรอยของปัญหาที่เกิดขึ้น ตัวอย่างเช่น Hacker มักจะอาศัยประตูหลังและ Proxy คอมพิวเตอร์ เมื่อทำการเข้าโจมตีเพื่อที่ทำการซ่อนร่องรอยและเพื่อใช้ประโยชน์จากโอกาสใดๆ ที่เปิดอยู่ เช่น ช่องว่างของระบบ NTP ซึ่งเป็นโอกาสที่

Hacker จะประสบตลอดเส้นทาง ดังนั้นการค้นหาจุดที่ทำการหยุดค้นหาจึงเป็นจุดสำคัญในการที่จะปิดประตูสำหรับการโจมตีครั้งต่อไป และต้องการจัดเวลาที่แม่นยำเพื่อเป็นการสร้างเลียนแบบขึ้นมาใหม่ของกระบวนการของเหตุผลที่เกิดขึ้น

Log file และการประทับเวลาที่ Application จึงเป็นสิ่งที่เห็นได้ชัดเจนว่าเป็นหลักฐานชิ้นสำคัญแน่นอนว่านี้เป็นชิ้นส่วนเดียวกันกับที่ใช้ในการตรวจสอบปัญหาของระบบ โดยทั่วไปไม่ใช่เฉพาะกรณี ที่มีการถูกแทรกแซงโดย Hacker เนื่องจากโดยปกติ Network Log File จะประกอบด้วยเวลาที่ประทับลงไปจากเครื่องต่างๆกัน ผู้บริหารระบบจึงสามารถใช้มันในการสร้างเหตุการณ์ย้อนหลังเพื่อนำไปสู่การเกิดเหตุใดๆ ใน Network

ข้อมูลทางสถิติที่เกี่ยวข้องกับ Performance ของ Network สามารถถูกบันทึกและนำมาวิเคราะห์ ทำให้ผู้บริหารระบบสามารถแยกแยะกระบวนการที่เป็นคอขวดและโอกาสอื่นๆ เพื่อทำการทำระบบให้ดีที่สุด ทั้งหมดเหล่านี้เห็นได้ชัดเจนว่าขึ้นอยู่กับว่าเวลาที่ประทับลงไปได้ถูก Synchronize

การจัดหา Network Time ที่ถูกต้อง

มีอยู่ 2 ลักษณะที่ทำให้การรักษาเวลาของ Network เป็นเรื่องง่าย

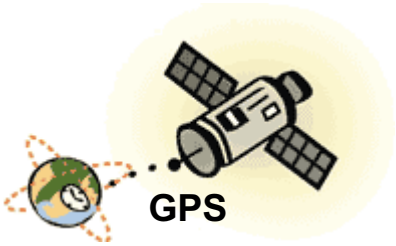
1. การที่เวลาของคอมพิวเตอร์แต่ละเครื่องจะถูกประสาน (synchronize) เข้ากับแม่ข่าย time server

2. กำจัดความต้องการที่จะต้องออกนอก Firewall เพื่อจะทำการ synchronize เวลาเข้ากับ Time Source ภายนอก ยังมีผลประโยชน์อย่างอื่นที่มาจากการใช้ time server เช่นเดียวกัน ซึ่งจะขึ้นอยู่กับคุณลักษณะของ server ที่ถูกติดตั้ง ซึ่งประโยชน์ต่างๆ เหล่านี้ไม่มีแน่นอนหากทำการ synchronize เวลาโดยผ่านอินเตอร์เนทจากแม่ข่าย NTP สาธารณะ

บทสรุปที่สำคัญของ Time Server

Time Source ที่แม่นยำ

แน่นอนว่าสิ่งที่สำคัญที่สุดที่จะได้จาก Time Source ก็คือเวลาที่แม่นยำที่มีส่วนประกอบอยู่ 3 ส่วน ที่ทำให้เกิดความแม่นยำ คือ ตัว Time Source เอง การเปิดให้เข้าถึงต่อ Time Source และความน่าเชื่อถือของ Time Server ในการรักษาเวลาที่แม่นยำ หลังจากที่มันได้รับเวลาที่ถูกต้องจาก Time Source โดยนิยามเวลาที่แม่นยำ คือ เวลาที่ผ้องกับเวลา UTC ซึ่งเป็นมาตรฐานเวลาที่ได้รับการยอมรับทั่วโลก เวลา UTC ได้จากสถาบันการวัดแห่งชาติของประเทศต่างๆ เช่น NIST ใน สหรัฐอเมริกา เวลา UTC สามารถได้รับจาก NIST ได้ สองถึงสามวิธีการ คือ โดยการหมุนโทรศัพท์ไปที่ NIST NTP Server หรือโดยการส่งสัญญาณคลื่นวิทยุ WWVB นอกจากนี้ UTC ยังสามารถรับได้ผ่านทางระบบดาวเทียม GPS ซึ่งควบคุมโดย USNO (United State Naval Observatory) UTC นั้นสามารถหาได้จากแหล่งต่างๆบนอินเตอร์เน็ท แต่ Time Source ที่ผ่านระบบอินเตอร์เน็ทจะสร้างปัญหาเรื่องความปลอดภัยตามที่ได้กล่าวถึงมาก่อนหน้า และยังมีปัญหาของการเดินทางของข้อมูลซึ่งก็คือ การหน่วงของเวลาจากการที่ Time package ออกจาก Time Source และใช้เวลาในการเดินทางก่อนที่จะมาถึง Network การลดระยะเวลาเดินทางให้น้อยที่สุดจะเป็นการทำให้ความแม่นยำของการ synchronization ดีที่สุด



Time Source สำรอง

Server ที่มีคุณภาพที่ดีกว่า คือเครื่องที่สามารถรับเวลาจาก Source หลายแหล่งไม่ใช่เพียงแหล่งเดียว Time Source สำรองหมายถึง Time Server สามารถทำการเลือกเส้นทางไปยังแหล่งอื่นๆ ตามความจำเป็นที่เกิดขึ้น เช่นเมื่อบริษัททำการเคลื่อนย้ายหรือเปลี่ยนแปลงโครงสร้าง Network

การประสานเวลาที่น่าเชื่อถือ

แน่นอนหลังจากทำการประสาน (sync) กันอยู่ Universal Time (UTC) Sever ก็จะกลายเป็น Time Source สำหรับ Network วิธีการที่ Time Server ทำงานจะเป็นดังต่อไปนี้

คอมพิวเตอร์แต่ละเครื่องใน Network จะส่งคำร้องขอไปยัง Time Server เพื่อขอเวลาที่แม่นยำโดยการเปรียบเทียบเวลาของคอมพิวเตอร์ที่ร้องขอกับเวลาของ Time Server และนับรวมถึงการ delay ของ Network เวลาของคอมพิวเตอร์ที่ร้องขอจะสามารถถูกตั้งให้เข้ากับเวลาของ Time server ได้ ปัจจัยสำคัญที่มีผลกระทบต่อความน่าเชื่อถือของ Time server คือ ความแม่นยำของ Clock ภายใน Time Server หาก Clock มีความแม่นยำ Time server สามารถทิ้งช่วงเวลาในการขอ ซิงค์กับ UTC ในแต่ละครั้งโดยยังคงความแม่นยำอยู่ได้

Rubiduim Clock เป็นอุปกรณ์ชนิดที่ใช้ใน GPS Satellite รุ่นใหม่ๆ เป็น Clock ที่แม่นยำที่สุดที่มีใช้ใน Network Time Server สำหรับทางด้านการค้าทั่วไปซึ่งจะสามารถรักษาความแม่นยำ หนึ่งในล้านของวินาทีต่อวัน ซึ่งเป็นระดับที่ยอมรับได้ สำหรับ Software ที่เกี่ยวข้องกับเวลาหากจะเปรียบเทียบ Protocol ของ Windows 2000 คือ MIT Turbo Loss Version 5 กำหนดไว้ว่า Network domain controller จะต้องปฏิบัติงานโดยมีความแตกต่างของเวลาภายในไม่เกิน 5,000 millisecond จึงจะอนุญาตให้ทำการ log on ระหว่าง controller ได้

Time Source ที่ปลอดภัย

ความปลอดภัยที่เพิ่มขึ้นคือสิ่งที่ได้มาโดยอัตโนมัติหากทำงานหลัง Firewall

ความง่ายในการใช้งาน

ด้วยการติดตั้งแบบ Plug and Play ของ Network Time Server และหลังจากตั้งเครื่องครั้งแรก ลืมได้เลยว่าต้องคอยดูแลบำรุงรักษาเหมือน Server โดยทั่วไป การตั้ง configuration ของ Network เป็นเพียงการเสียบ Server เข้ากับ Network ผ่านทางสายแลนมาตรฐาน การตั้งเวลาทำเพียงครั้งเดียว เพียงแต่เสียบสายอากาศ GPS หรือทำการหมุนโมเด็มข Server จะทำการค้นหาสัญญาณดาวเทียมโดยอัตโนมัติ หรือทำการต่อหมายเลขเพื่อทำการต่อสายเท่านั้น ระบบก็สามารถทำงานได้ทันที

ประสิทธิภาพของต้นทุน

Time Server เป็นสิ่งที่เป็นการลงทุนที่คุ้มค่าในการเพิ่มความน่าเชื่อถือประสิทธิภาพและความปลอดภัยของ Network.Time Server เครื่องหนึ่งมีราคาไม่เกิน แต่สามารถให้บริการต่อคอมพิวเตอร์เป็นพันๆเครื่องใน Network

บทสรุป

เมื่อผู้บริหารในทุกวันนี้พูดคุยกันถึงการบริหารเวลา หรือการปฏิบัติการบน Internet Time พวกเขาอาจจะไม่ได้คิดถึงความเป็นจริงเบื้องหลังคำพูดเหล่านั้น

...Network Time Servers...