การทดลองที่ 23 เรื่องความปลอดภัยในการสื่อสารแบบ VoIP

23.1. วัตถุประสงค์ในการทดลอง

1.1 เพื่อศึกษาถึงความไม่ปลอดภัยของการส่งข้อมูลเสียงบนโพรโทคอล SIP และ RTP

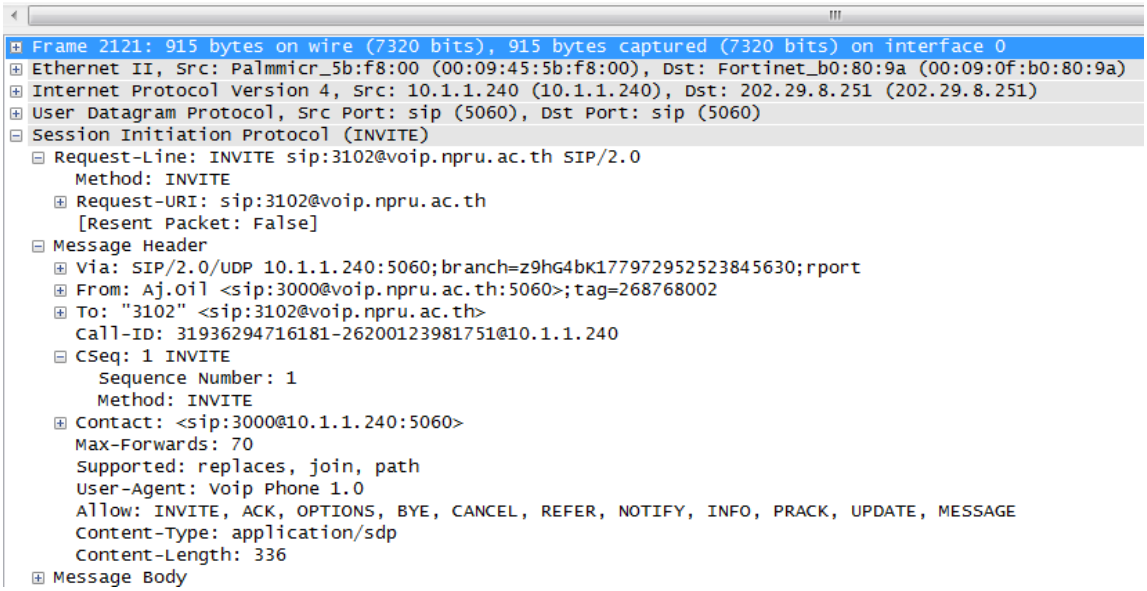
1.2 เพื่อศึกษาแนวทางการเข้ารหัสสัญญาณเสียงก่อนส่งออกสู่เครือข่ายคอมพิวเตอร์ด้วยโพรโทคอล TLS และ SRTP

23.2. หลักการและทฤษฎีที่เกี่ยวข้อง

ในการสื่อสารด้วยโพรโทคอลSIP และ RTP นั้นจะไม่มีการเข้ารหัสข้อมูล ดังนั้นแพ็กเก็ตข้อมูลจะถูกส่งออกไปเป็นแบบ Plaintext หากมีผู้ไม่หวังดีทำการโจมตีข้อมูล เช่น ดักฟังเปลี่ยนแปลงข้อมูลก็จะก่อให้เกิดความเสียหายได้ ดังนั้นในการทดลองนี้ผู้เรียนจะได้ศึกษาถึงความไม่ปลอดภัยของการส่งข้อมูลด้วย SIP และ RTP นอกจากนั้นผู้เรียนยังจะได้ทำการศึกษาถึงแนวทางการเข้ารหัสสัญญาณก่อนส่งออกสู่เครือข่ายโดยโพรโทคอลTLS และ STRP อีกด้วย

2.1 ความไม่ปลอดภัยของการส่งสัญญาณควบคุมด้วย SIPและ RTP

รูปที่ 1 แสดงให้เห็นรายละเอียดของแพ็กเก็ต INVITE ใน SIP ซึ่งสามารถใช้ Wiresharkในการตรวจจับแพ็กเก็ตดังกล่าว โดยรายละเอียดมีดังนี้



รูปที่ 1 SIP INVITE packet

Request-Line: บอกชนิดของการร้องขอว่าเป็น ชนิดใด เช่น INVITE, ACK, CANCEL, BYE เป็นต้น ซึ่งในกรณีตัวอย่างนี้ เป็นการร้องขอชนิด **INVITE** ใช้เพื่อขอเชื่อมต่อการสื่อสาร โดยที่ URI ที่ต้องการ

เชื่อมต่อด้วย คือ 3102@voip.npru.ac.thและโพรโทคอลSIP **ที่ใช้คือ เวอร์ชั่น 2** ในส่วนที่เหลือจะเป็นส่วนรายละเอียดของ header

- Via: รายละเอียดของไอพีแอดเดรสของผู้โทรต้นทาง 10.1.1.240 และเป็นที่อยู่ซึ่งรอการตอบสนองจากฝั่งผู้รับปลายทางในกรณีที่แพ็กเก็ตต้องเดินทางหลายฮอปก่อนจะถึงผู้รับสายปลายทาง ไอพีแอดเดรสของ proxy server ของฮอปต่างๆ จะถูกเก็บไว้ใน Via ด้วย เพื่อให้แพ็กเก็ตจากผู้รับปลายทางสามารถเดินทางกลับมาหาผู้พูดต้นทางได้ (หมายเหตุ ข้อมูลใน Via จะใช้ในการส่งแพ็กเก็ตเพื่อตอบสนองของการร้องขอจากผู้โทรต้นทาง)

- Max-Forward : ตัวเลขจำนวนเต็มที่ใช้กำหนดจำนวนฮอบการเดินทางของการร้องขอนี้ว่าไม่ให้เกินกี่ฮอป (ในกรณีตัวอย่างนี้ คือ 70 ฮอป) หลักการทำงานของพารามิเตอร์ Max-Forward ก็คือ ในทุกๆ ฮอปการเดินทางก่อนถึงผู้รับปลายทาง ตัวเลขนี้จะถูกลดจำนวนลงทีละ 1 ทั้งนี้เพื่อป้องกันกรณีการเกินลูปภายในเครือข่าย

- To : รายละเอียดของผู้รับปลายทาง

- From : รายละเอียดของผู้โทรต้นทาง นอกจากนั้นยังมีส่วนของ tag ที่เป็นหมายเลขแบบสุ่ม ที่ใช้ในการแยกแยะการเชื่อมต่อ

- Call-ID : หมายเลขที่สร้างขึ้นจากการผสมผสานระหว่างตัวเลขแบบสุ่มกับไอพีแอดเดรส โดยที่ Call-ID ในแต่ละครั้งของการโทรนั้นจะไม่ซ้ำกัน (หมายเหตุ การแต่ละครั้งของการโทรนั้น อาจมีได้หลายการเชื่อมต่อ)

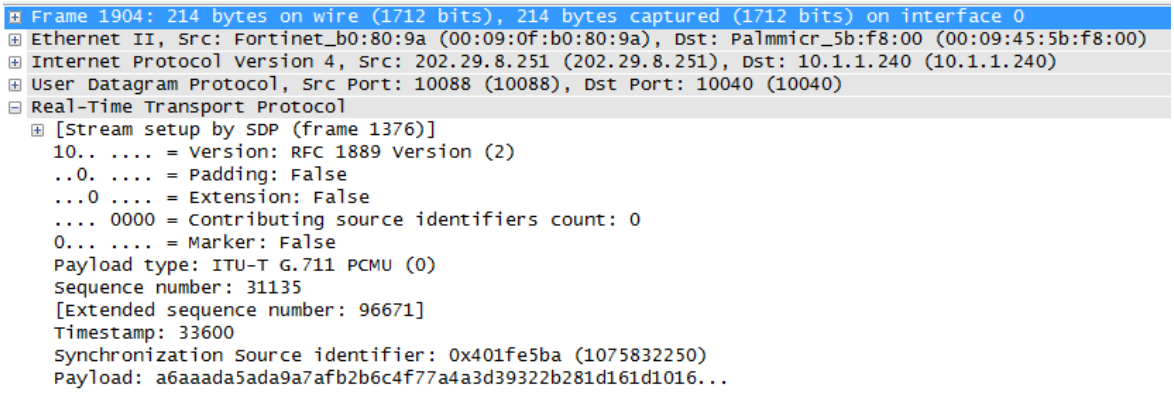
- CSeq : ประกอบไปด้วยเลขจำนวนเต็ม และชนิดของการร้องขอ (ในที่นี้คือ INVITE) ในตอนเริ่มต้นของการเชื่อมต่อ ค่าของเลขจำนวนเต็มจะถูกกำหนดขึ้นอย่างสุ่ม แล้วจะถูกเพิ่มค่าขึ้นทีละ 1 สำหรับทุกๆ แพ็กเก็ตที่มีการติดต่อระหว่างผู้โทรต้นทางและปลายทาง ค่าตัวเลขจำนวนเต็มนี้จะช่วยบอกได้ว่า มีการสูญหายของแพ็กเก็ตบ้างหรือไม่ และยังช่วยในการจัดลำดับก่อนหลังของแพ็กเก็ต

- Contact : รายละเอียดของการติดต่อไปยังผู้เรียกต้นทางโดยตรง (ไม่ต้องผ่านเครื่องแม่ข่าย) ความแตกต่างระหว่างรายละเอียดที่อยู่ใน Via กับ Contact คือ ข้อมูลที่อยู่ใน Contact จะถูกใช้ในการส่งแพ็กเก็ตต่อไป

- Allow : ชนิดของการร้องขอที่ฝั่งผู้โทรต้นทางยอมรับได้ โดยใน SIP จะมีชนิดของการร้องขอ ดังนี้ ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, PRACK, REFER, REGISTER, SUBSCRIBE, UPDATE จะเห็นได้ว่าการใช้ SIP ในการส่งสัญญาณควบคุมเพื่อเชื่อมต่อการสื่อสารนั้น หากผู้บุกรุกสามารถดักจับแพ็กเก็ตต่างๆ ในระหว่างการเชื่อมต่อ ผู้บุกรุกก็จะมีข้อมูลที่เกี่ยวข้องทั้งของผู้โทรต้นทาง และผู้โทรปลายทางซึ่งจะสามารถนำไปใช้ในการบุกรุกรูปแบบอื่นๆ ต่อไปได้

ในส่วนของการส่งข้อมูลการสนทนาผ่านโพรโทคอลRTP นั้น หากมองในระดับแพ็กเก็ตแล้ว (ดูรูปที่ 2) จะพบว่ามีข้อมูลของ Codec, Sequence number และส่วนของ payload ซึ่งหากผู้บุก

รุกสามารถดักจับกระแส RTP ของการสนทนาได้ ก็สามารถนำข้อมูลดังกล่าวมาประกอบกัน และถอดรหัส Codec ที่ถูกต้องออกมาเพื่อแอบฟังการสนทนาได้



รูปที่ 2 RTP packet

2.2 แนวทางการเข้ารหัสสัญญาณก่อนส่งออกสู่เครือข่ายโดยโพรโทคอลTLS และ SRTP

เนื่องจากปัญหาของความไม่ปลอดภัยต่อการดักฟังของการใช้โพรโทคอลSIP และ RTP ในการใช้งานระบบ VoIP ทำให้มีการพัฒนาโพรโทคอลTLS และ SRTP เพื่อใช้ในการส่งสัญญาณควบคุมและสัญญาณเสียงแบบเข้ารหัส ดังนั้นถึงแม้ว่าผู้บุกรุกจะสามารถดักจับแพ็กเก็ตของโพรโทคอลดังกล่าวได้ ก็ไม่สามารถเข้าใจว่ามีข้อมูลใดอยู่ภายในแพ็กเก็ตบ้าง

Transport Layer Security (TLS) หรือชื่อเดิม Secure Sockets Layer (SSL) เป็นโพรโทคอลที่ใช้เข้ารหัสข้อมูลที่ส่งในอินเทอร์เน็ต เช่น เว็บเพจ จดหมายอิเล็กทรอนิกส์ โปรแกรมสนทนา และอื่นๆ เพื่อความปลอดภัยในการส่งข้อมูล มีข้อแตกต่างในรายละเอียดทางเทคนิคระหว่าง SSL 3.0 และ TLS 1.0 เพียงเล็กน้อย ดังนั้นตัวย่อ SSL จะหมายถึงโพรโทคอลทั้งคู่ ในกรณีที่ไม่ระบุว่าตัวใดตัวหนึ่งเป็นพิเศษ

SRTP คือรูปแบบการส่งข้อมูลมัลติมีเดียซึ่งจะทำการทำงานโดยการเข้ารหัสข้อมูล ช่วยในเรื่องของความมั่นคงปลอดภัยโดยนำมาใช้ใน VoIP โดยเฉพาะการส่งข้อมูลในระดับบิต เพราะสามารถใช้กับการบีบอัดส่วนหัวและไม่มีผลกระทบต่อคุณภาพการให้บริการ ในการส่งข้อมูลมัลติมีเดีย SRTP จะใช้งานได้อย่างมีประสิทธิภาพทั้งในเครือข่ายแบบมีสายและไร้สาย SRTP เป็นโพรโทคอลทางด้านความปลอดภัย โดยมีการสร้างแพ็กเก็ตSRTP แล้วส่งต่อแพ็กเก็ตนี้ไปถึงผู้รับในทำนองเดียวกันฝั่งผู้รับก็ทำการถอดรหัสแพ็กเก็ตที่รับมา ซึ่งก็จะทำให้การสื่อสารมีความมั่นคงปลอดภัยไม่สูญเสียความลับในการติดต่อสื่อสาร

23.3. อุปกรณ์การทดลอง

3.1 เครื่องโทรศัพท์ไอพี	จำนวน	1 เครื่อง
3.2โทรศัพท์ชนิด Softphone (X-lite)	จำนวน	1 เครื่อง
3.3 โทรศัพท์ชนิด Softphone (Blink)	จำนวน	1 เครื่อง
3.4 IP-PBX ทำหน้าที่เป็น server	จำนวน	1 เครื่อง
3.5 เครื่องคอมพิวเตอร์โน๊ทบุคติดตั้ง Blink (นักศึกษาเตรียมมาเอง)	จำนวน	1 เครื่อง

23.4. ขั้นตอนการทดลองและผลการทดลอง

4.1 ความไม่ปลอดภัยของ SIP และ RTP ต่อการดักฟัง

4.1.1 ทำการคอนฟิคเครื่องซอฟต์โฟนX-lite ให้มีรายละเอียด ดังนี้

- User ID: 1001
- Domain: 10.1.77.227 (หรือค่าไอพีแอดเดรสของเครื่อง IP-PBX)
- Password: password1001

4.1.2 ทำการคอนฟิคเครื่องโทรศัพท์ไอพี ให้มีรายละเอียด ดังนี้

- SIP Protocol Settings:

  Account: 1002

  PIN: password1002

  User Service: enable

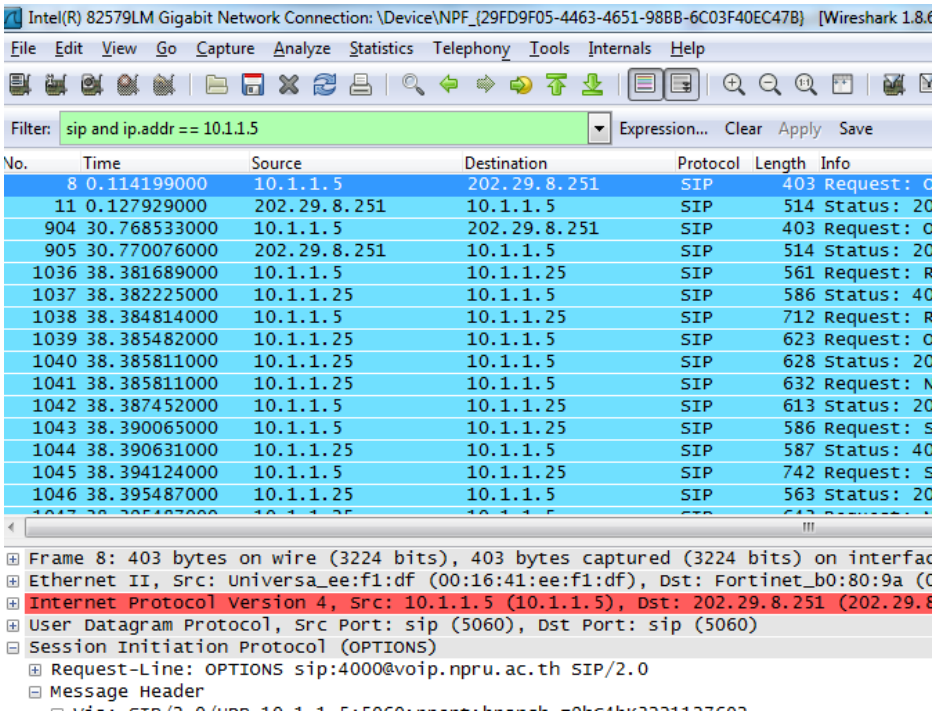
  Register port: 5060

4.1.3 เปิด Wiresharkเพื่อทำการ Capture packet

4.1.4 โทรจากเบอร์ 1001 (X-lite) ไปหา 1002 (เครื่องโทรศัพท์ไอพี) แล้วทำการรับสาย ทำการสนทนาสัก 30 วินาที แล้วให้เบอร์ 1001 วางสาย

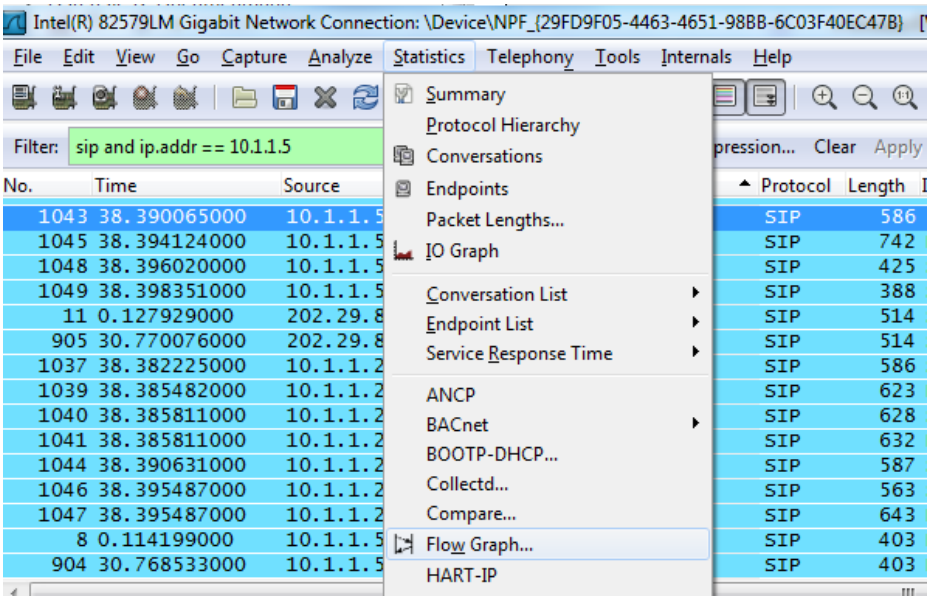
4.1.5 ปิดการ Capture ของ Wireshark

4.1.6 ในWiresharkช่อง Filter ใส่การกรอง “SIP and ip.addr==<ไอพีแอดเดรสของ X-lite>” ดังแสดงในรูปที่ 3 (กรณีนี้ไอพีแอดเดรสของ X-lite คือ 10.1.1.5)



รูปที่ 3 การกรองแพ็กเก็ตที่สนใจใน Wireshark

4.1.7 ไปที่ Toolbar ของ Wiresharkแล้วคลิก Statics->Flow Graph ดังแสดงในรูปที่ 4 จะปรากฏหน้าต่างย่อยขึ้นมาให้คลิ๊กOK แล้วบันทึกผลที่ได้



รูปที่ 4 การสร้าง Flow Graph

- ผลการทดลอง (แสดงเป็นรูป Flow graph)

.....

.....

.....

.....

.....

.....

.....

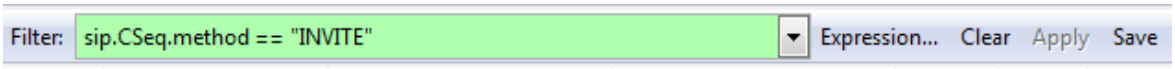
.....

.....

.....

.....

4.1.8 ในช่อง Filter ใส่ “sip.CSeq.method == “INVITE”” ดังแสดงในรูปที่ 5 เพื่อกรองเอาเฉพาะแพ็กเก็ตที่ทำการ INVITE



รูปที่ 5 การ Filter เพื่อกรองเอาเฉพาะแพ็กเก็ตที่ทำการ INVITE

- ผลการทดลอง

.....

.....

.....

.....

.....

.....

.....

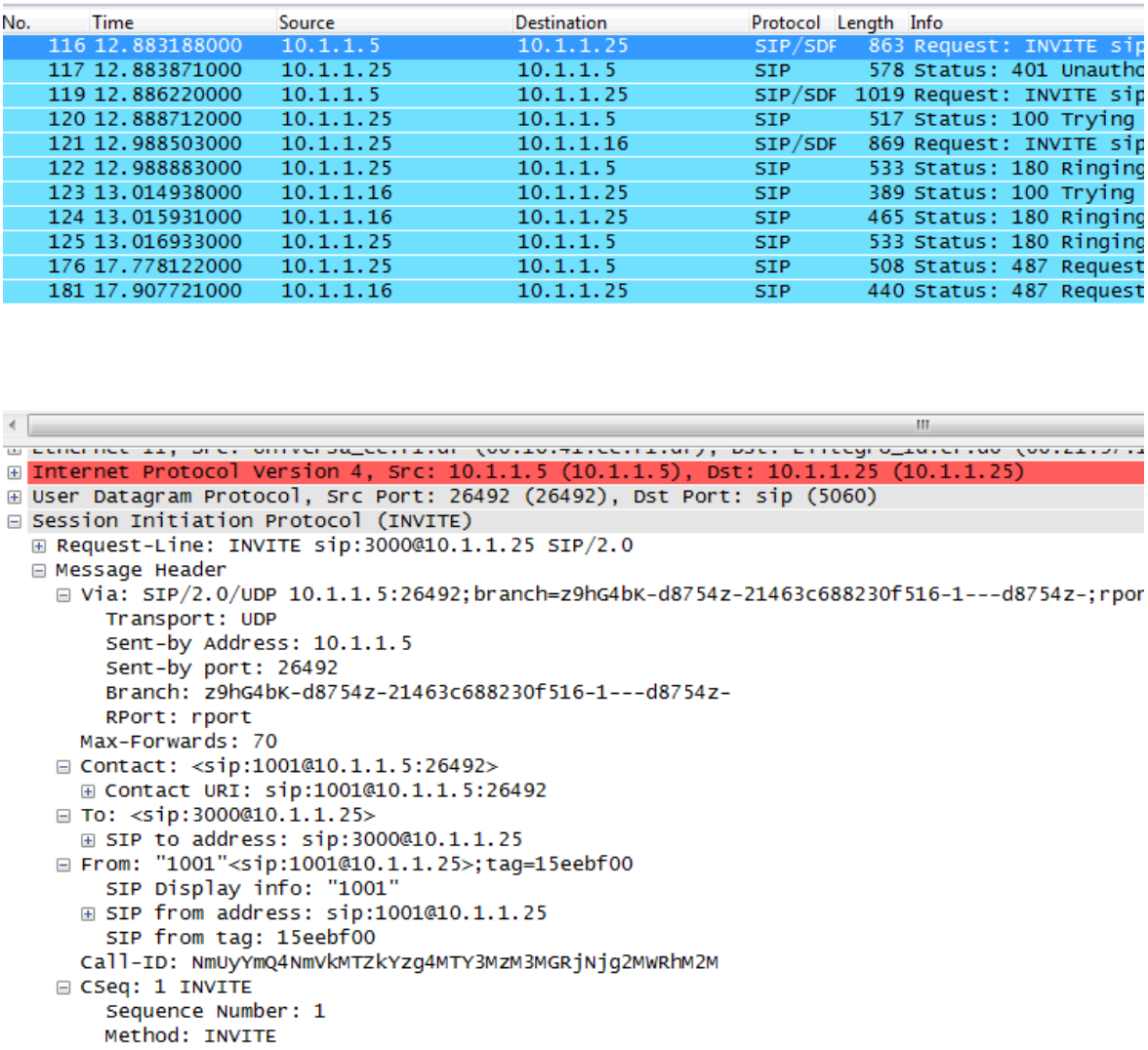
.....

.....

.....

.....

4.1.9 เลือกแพ็กเก็ตINVITE โดยทำการคลิ๊กบนแพ็กเก็ตนั้นๆ (จะเป็นแถบสีน้ำเงินเข้ม) ดังแสดงในรูปที่ 6



รูปที่ 6 รายละเอียดภายในแพ็กเก็ต INVITE

- ผลการทดลอง

.....

.....

.....

.....

.....

.....

4.1.10 กดปุ่ม Clear ที่แถบ Filter เพื่อลบการกรองทั้งหมด

4.1.11 ที่ Toolbar ->Telephony->VoIP Calls แล้วคลิ๊กเลือก Call ที่ต้องการดักฟัง แล้วกด Player->Decode (ให้เปิดเสียงที่ลำโพงของเครื่องโน้ตบุ๊คที่ติดตั้ง Wiresharkด้วย)

- ผลการทดลอง

.....

.....

.....

.....

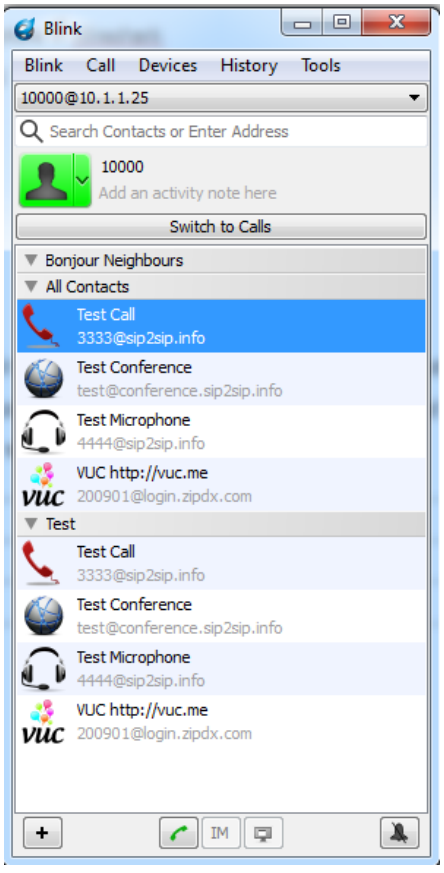
.....

.....

4.1.12 ปิดโปรแกรม X-lite

4.2 การเพิ่มความปลอดภัยในระบบ VoIP ด้วย TLS และ SRTP

4.2.1เปิดโปรแกรมซอฟต์โฟนBlinkซึ่งมีหมายเลขโทรศัพท์ คือ 10000 (หมายเลขนี้ถูกติดตั้งให้ใช้โพรโทคอลTLS และ SRTP ในการเชื่อมต่อการสนทนา)

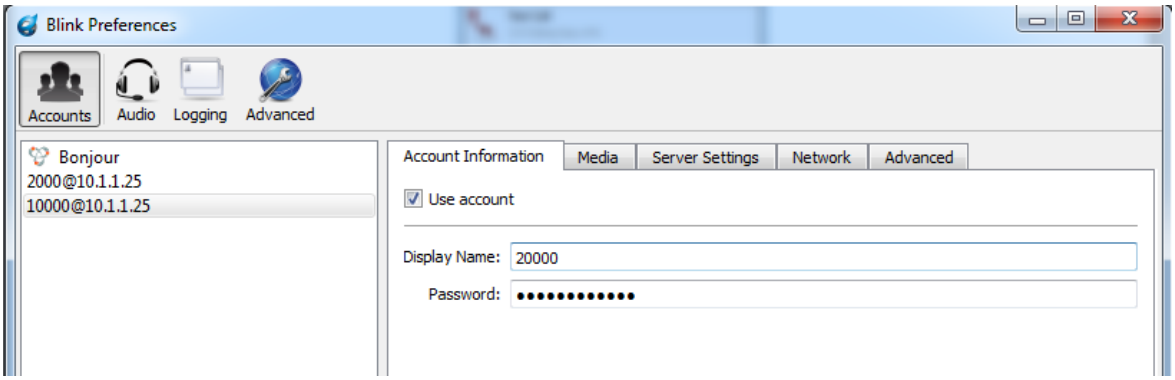


รูปที่ 7 Blink Softphone

4.2.2 เปิดโปรแกรมซอฟต์โฟนBlink ในเครื่องโน้ตบุ๊คอีกเครื่องแล้วทำการคอนฟิคค่าโทรศัพท์ เบอร์ 20000 ดังนี้

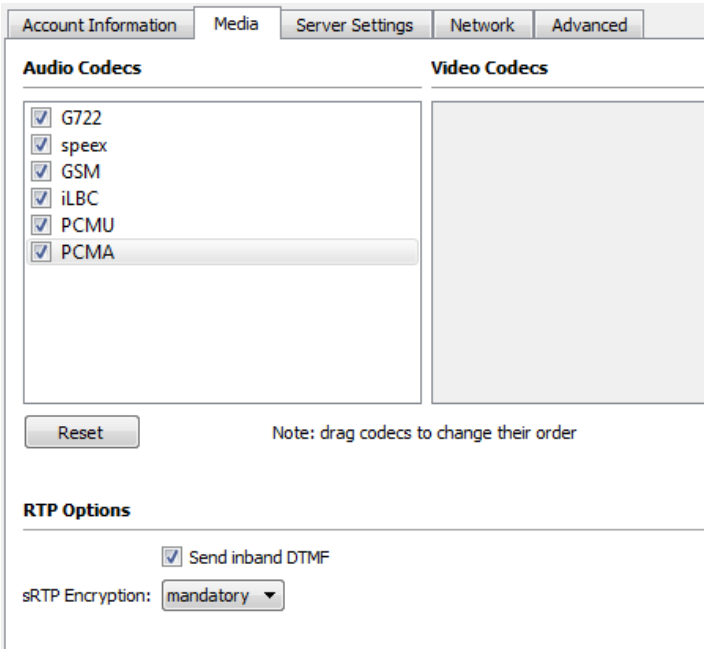
4.2.2.1 แทบ Account Information

- Display Name: 20000
- Password: password20000



รูปที่ 8 การ Set up Username และ Password ใน Blink softphone เครื่องที่ 1

4.2.2.2 แทบ Media เซตค่า sRTP Encryption: Mandatory



รูปที่ 9 การเซตค่า sRTP Encryption ใน Blink softphone

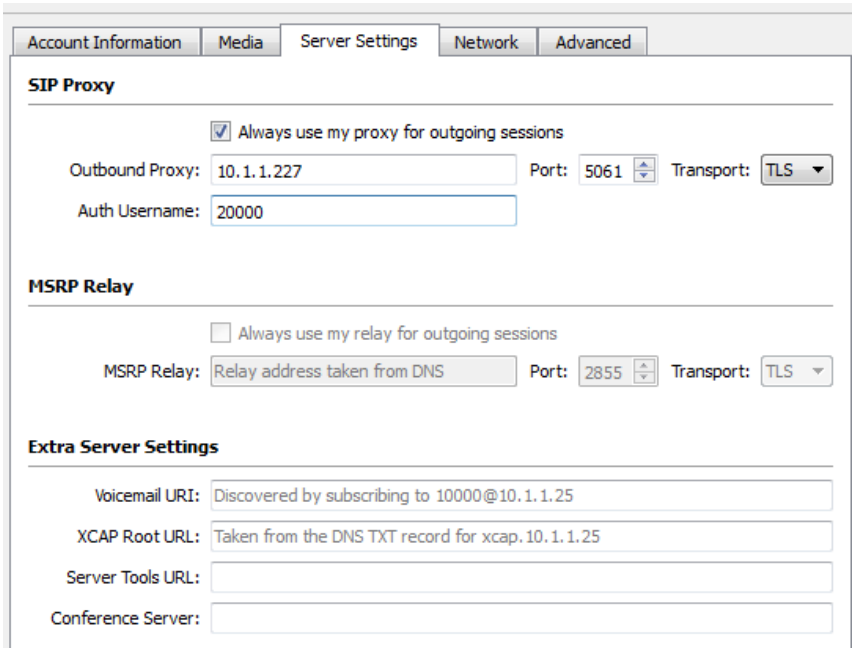
4.2.2.3 แทบ Server Settings ใส่รายละเอียดของ IP-PBX

Outbound Proxy: 10.1.1227

Port: 5061

Transport: TLS

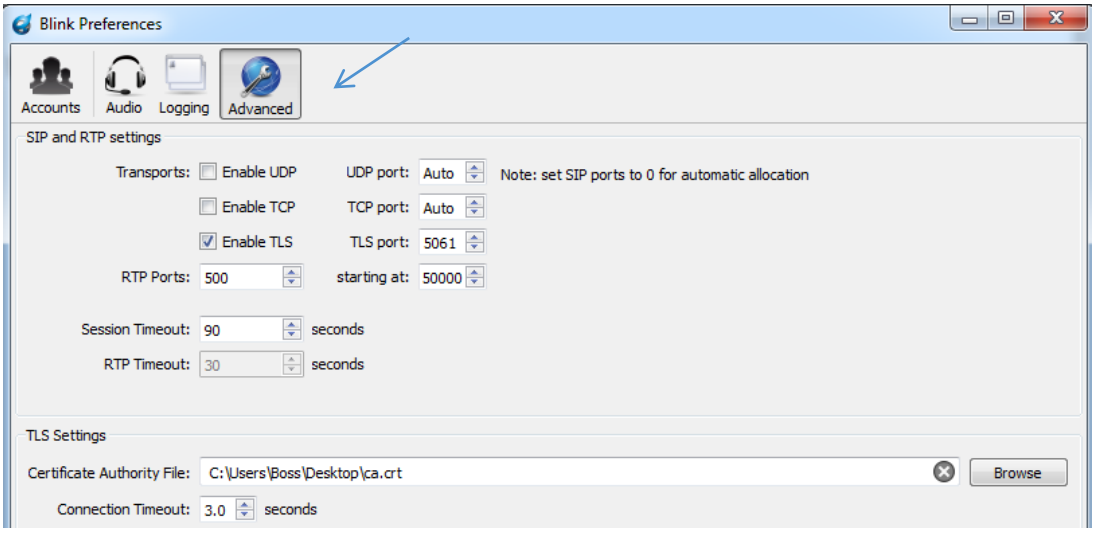
Auth Username: 20000



รูปที่ 10 การเซตค่าเกี่ยวกับ IP – PBX

4.2.2.4 แถบเมนู เลือก Advanced

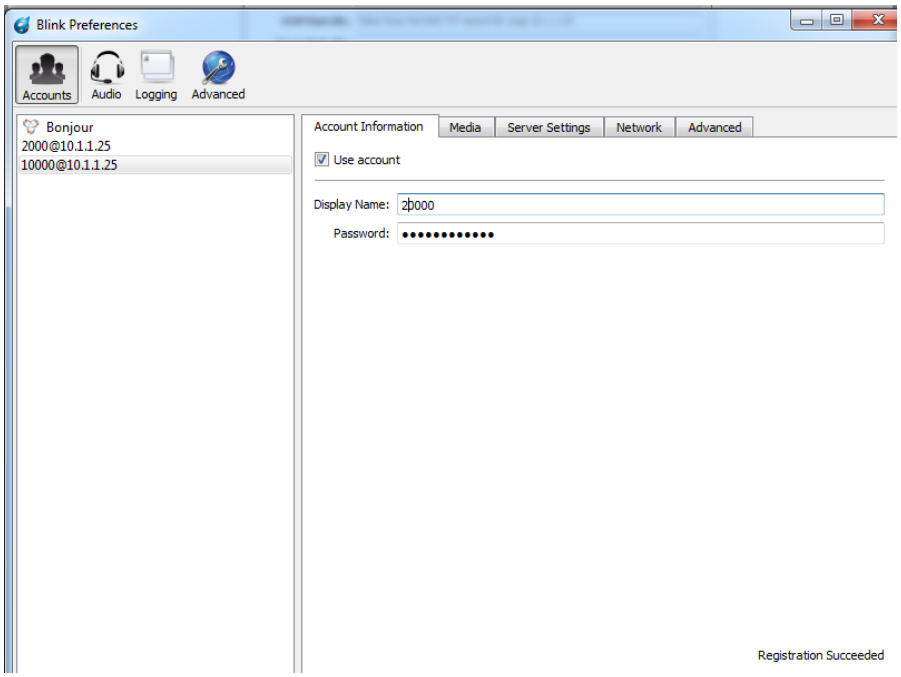
- Enable TLS
- เลือกไฟล์ ca.crt บนหน้าเดสก์ทอป ใส่เข้าไปใน Certificate Authority File



รูปที่ 11 การเซตค่า Enable TLS

4.2.2.5 ที่แถบเมนู เลือก Accounts-> Account Information

หากลงทะเบียนสำเร็จ จะพบ Registration Succeeded ด้านล่าง



รูปที่ 12 การ Set up Username และ Password ใน Blink softphone เครื่องที่ 2

4.2.2.6 ปิดหน้าจอของการติดตั้ง

4.2.3 ทำการเปิดการ capture ที่ Wireshark

4.2.4 โทรจาก 10000 ไปหาเบอร์ 20000 แล้วทำการสนทนาประมาณ 30 วินาที แล้วให้เบอร์ 10000 วางสาย

4.2.5 ปิดการ Capture ของ Wireshark

4.2.6 ในหน้าจอWireshark ปรากฏโพรโทคอล อะไรบ้าง มี โพรโทคอลSIP บ้างหรือไม่อย่างไร

-ผลการทดลอง

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

4.2.7 ไปที่ Toolbar ของ Wireshark แล้วคลิก Statics->Flow Graph จะปรากฏหน้าต่างย่อยขึ้นมาให้คลิ๊ก OK แล้วบันทึกผลที่ได้

-ผลการทดลอง

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

4.2.8 ที่ Toolbar ->Telephony->VoIP Calls แล้วคลิ๊กเลือก Call ที่ต้องการดักฟัง แล้วกด Player->Decode (ให้เปิดเสียงที่ลำโพงของเครื่องโน้ตบุคที่ติดตั้ง Wireshark ด้วย)

-ผลการทดลอง

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

23.5. สรุปผลการทดลอง

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

23.6. คำถามท้ายการทดลอง

1. ในการโทรศัพท์ด้วยการใช้โพรโทคอล SIP และ RTP นั้นเหตุใดจึงไม่ปลอดภัยต่อการดักดับข้อมูล ให้อธิบายรายละเอียดถึงข้อมูลอะไรบ้าง ที่จะสามารถถูกดักจับได้

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. หลักการเข้ารหัสของ TLS และ SRTP เป็นอย่างไร (ใช้แบบกุญแจเดียว หรือ กุญแจสาธารณะจงอภิปราย)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. ในการโพรโทคอล TLS และ SRTP นั้นหากแพ็กเก็ตข้อมูลถูกดักจับ จะมีข้อมูลอะไรบ้างที่ผู้บุกรุกสามารถขโมยได้

.....

.....

.....

.....

.....

.....

.....