

การทดลองที่ 23 เรื่องความปลอดภัยในการสื่อสารแบบ VoIP

23.1. วัตถุประสงค์ในการทดลอง

- 1.1 เพื่อศึกษาถึงความปลอดภัยของการส่งข้อมูลเสียงบนโพรโทคอล SIP และ RTP
- 1.2 เพื่อศึกษาแนวทางการเข้ารหัสสัญญาณเสียงก่อนส่งออกสู่เครือข่ายคอมพิวเตอร์ด้วยโพรโทคอล TLS และ SRTP

23.2. หลักการและทฤษฎีที่เกี่ยวข้อง

ในการสื่อสารด้วยโพรโทคอล SIP และ RTP นั้นจะไม่มีมีการเข้ารหัสข้อมูล ดังนั้นแพ็กเก็ตข้อมูลจะถูกส่งออกไปเป็นแบบ Plaintext หากมีผู้ไม่หวังดีทำการโจมตีข้อมูล เช่น ดักฟังเปลี่ยนแปลงข้อมูลก็จะก่อให้เกิดความเสียหายได้ ดังนั้นในการทดลองนี้ผู้เรียนจะได้ศึกษาถึงความปลอดภัยของการส่งข้อมูลด้วย SIP และ RTP นอกจากนั้นผู้เรียนยังจะได้ทำการศึกษาถึงแนวทางการเข้ารหัสสัญญาณก่อนส่งออกสู่เครือข่ายโดยโพรโทคอล TLS และ STRP อีกด้วย

2.1 ความปลอดภัยของการส่งสัญญาณควบคุมด้วย SIP และ RTP

รูปที่ 1 แสดงให้เห็นรายละเอียดของแพ็กเก็ต INVITE ใน SIP ซึ่งสามารถใช้ Wireshark ในการตรวจจับแพ็กเก็ตดังกล่าว โดยรายละเอียดมีดังนี้

```

Frame 2121: 915 bytes on wire (7320 bits), 915 bytes captured (7320 bits) on interface 0
Ethernet II, Src: Palmmicr_5b:f8:00 (00:09:45:5b:f8:00), Dst: Fortinet_b0:80:9a (00:09:0f:b0:80:9a)
Internet Protocol Version 4, Src: 10.1.1.240 (10.1.1.240), Dst: 202.29.8.251 (202.29.8.251)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:3102@voip.npru.ac.th SIP/2.0
    Method: INVITE
    Request-URI: sip:3102@voip.npru.ac.th
      [Resent Packet: False]
  Message Header
    Via: SIP/2.0/UDP 10.1.1.240:5060;branch=z9hG4bk177972952523845630;rport
    From: Aj.Oil <sip:3000@voip.npru.ac.th:5060>;tag=268768002
    To: "3102" <sip:3102@voip.npru.ac.th>
    Call-ID: 31936294716181-26200123981751@10.1.1.240
    CSeq: 1 INVITE
      Sequence Number: 1
      Method: INVITE
    Contact: <sip:3000@10.1.1.240:5060>
    Max-Forwards: 70
    Supported: replaces, join, path
    User-Agent: Voip Phone 1.0
    Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, REFER, NOTIFY, INFO, PRACK, UPDATE, MESSAGE
    Content-Type: application/sdp
    Content-Length: 336
  Message Body
  
```

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.th และโพรโทคอล SIP ที่ใช้คือ เวอร์ชัน 2 ในส่วนที่เหลือจะเป็นส่วนรายละเอียดของ header

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

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

- 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 ในการส่งสัญญาณควบคุมเพื่อเชื่อมต่อสื่อสารนั้น หากผู้บุกรุกสามารถดักจับแพ็กเก็ตต่างๆ ในระหว่างการเชื่อมต่อ ผู้บุกรุกก็จะมีข้อมูลที่เกี่ยวข้องทั้งของผู้โทรต้นทาง และผู้โทรปลายทางซึ่งจะสามารถนำไปใช้ในการบุกรุกรูปแบบอื่นๆ ต่อไปได้

ในส่วนของการส่งข้อมูลการสนทนาผ่านโพรโทคอล RTP นั้น หากมองในระดับแพ็กเก็ตแล้ว (ดูรูปที่ 2) จะพบว่าข้อมูลของ Codec, Sequence number และส่วนของ payload ซึ่งหากผู้บุกรุก

เราสามารถดักจับกระแส RTP ของการสนทนาได้ ก็สามารถนำข้อมูลดังกล่าวมาประกอบกัน และถอดรหัส Codec ที่ถูกต้องออกมาเพื่อแอบฟังการสนทนาได้

```

Frame 1904: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
Ethernet II, Src: Fortinet_b0:80:9a (00:09:0f:b0:80:9a), Dst: Palmmicr_5b:f8:00 (00:09:45:5b:f8:00)
Internet Protocol Version 4, Src: 202.29.8.251 (202.29.8.251), Dst: 10.1.1.240 (10.1.1.240)
User Datagram Protocol, Src Port: 10088 (10088), Dst Port: 10040 (10040)
Real-Time Transport Protocol
  [Stream setup by SDP (frame 1376)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 31135
    [Extended sequence number: 96671]
    Timestamp: 33600
    Synchronization source identifier: 0x401fe5ba (1075832250)
    Payload: a6aaada5ada9a7afb2b6c4f77a4a3d39322b281d161d1016...
  
```

รูปที่ 2 RTP packet

2.2 แนวทางการเข้ารหัสสัญญาณก่อนส่งออกสู่เครือข่ายโดยโพรโทคอล TLS และ SRTP

เนื่องจากปัญหาของความไม่ปลอดภัยต่อการดักฟังของการใช้โพรโทคอล SIP และ RTP ในการใช้งานระบบ VoIP ทำให้มีการพัฒนาโพรโทคอล TLS 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 ในกรณีที่โม้ระบุว่าตัวใดตัวหนึ่งเป็นพิเศษ

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

23.3. อุปกรณ์การทดลอง

3.1 เครื่องโทรศัพท์ไอพี	จำนวน	1 เครื่อง
3.2 โทรศัพท์ชนิด 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 เครื่องคอมพิวเตอร์โน้ตบุ๊คติดตั้ง Blink (นักศึกษาเตรียมมาเอง)	จำนวน	1 เครื่อง

23.4. ขั้นตอนการทดลองและผลการทดลอง

4.1 ความไม่ปลอดภัยของ SIP และ RTP ต่อการดักฟัง

4.1.1 ทำการคอนฟิกเครื่องซอฟต์แวร์ X-lite ให้มีรายละเอียด ดังนี้

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

4.1.2 ทำการคอนฟิกเครื่องโทรศัพท์ไอพี ให้มีรายละเอียด ดังนี้

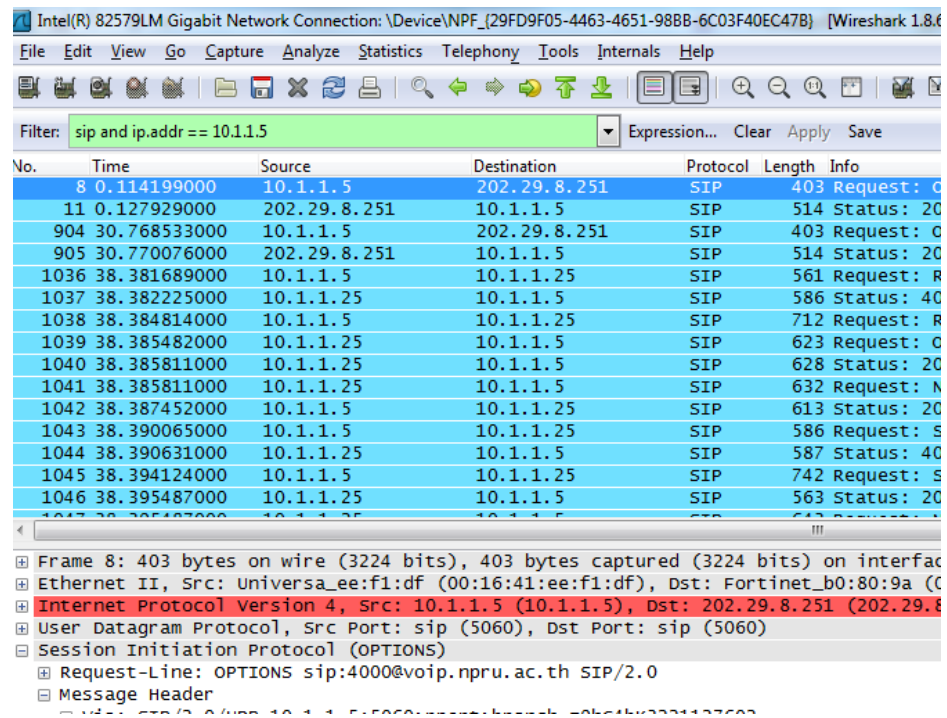
- SIP Protocol Settings:
 - Account: 1002
 - PIN: password1002
 - User Service: enable
 - Register port: 5060

4.1.3 เปิด Wireshark เพื่อทำการ Capture packet

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

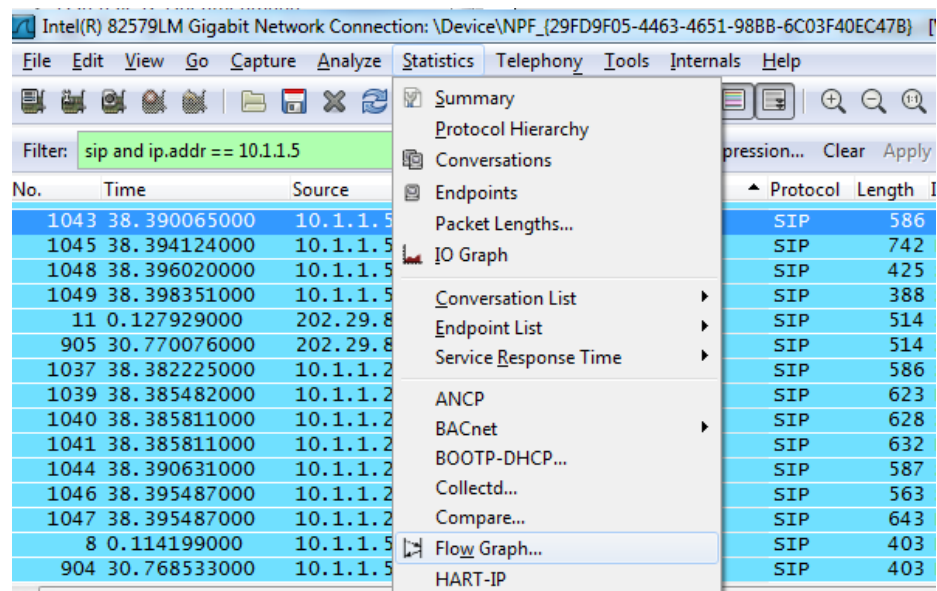
4.1.5 ปิดการ Capture ของ Wireshark

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



รูปที่ 3 การกรองแพ็กเก็ตที่สนใจใน Wireshark

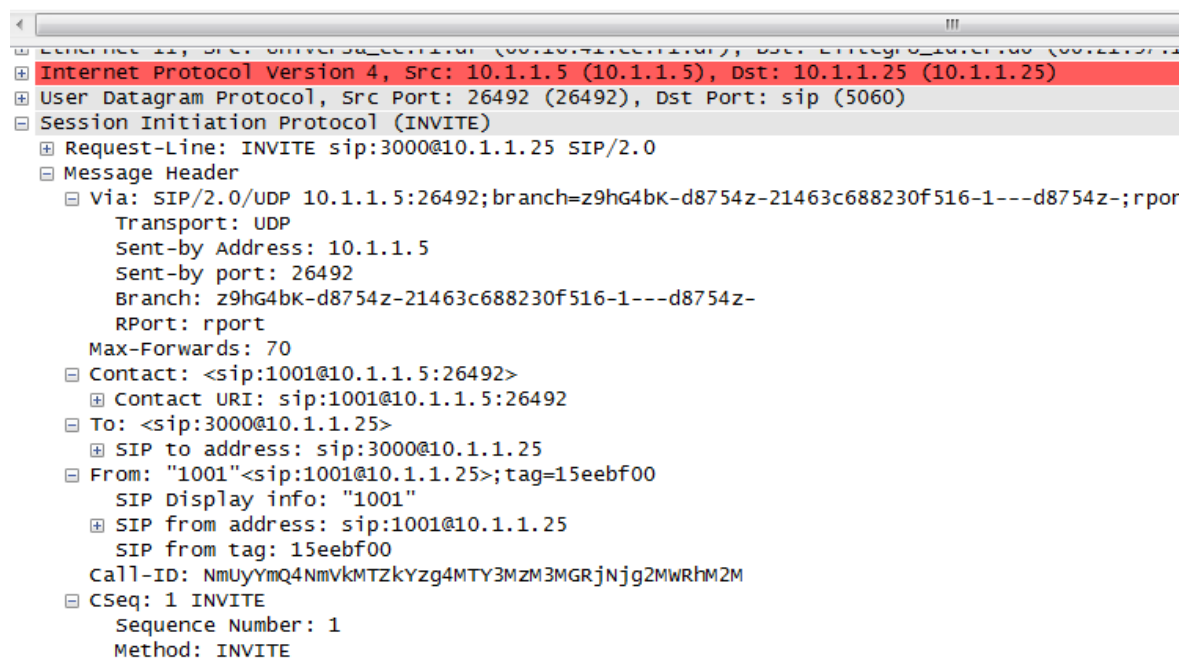
4.1.7 ไปที่ Toolbar ของ Wireshark แล้วคลิก Statics->Flow Graph ดังแสดงในรูปที่ 4 จะปรากฏหน้าต่างย่อยขึ้นมาให้คลิก OK แล้วบันทึกผลที่ได้



รูปที่ 4 การสร้าง Flow Graph

4.1.9 เลือกแพ็กเก็ตเกิดINVITE โดยทำการคลิกบนแพ็กเก็ตนั้นๆ (จะเป็นแถบสีน้ำเงินเข้ม) ดังแสดงในรูปที่ 6

No.	Time	Source	Destination	Protocol	Length	Info
116	12.883188000	10.1.1.5	10.1.1.25	SIP/SDF	863	Request: INVITE sip
117	12.883871000	10.1.1.25	10.1.1.5	SIP	578	Status: 401 Unauthc
119	12.886220000	10.1.1.5	10.1.1.25	SIP/SDF	1019	Request: INVITE sip
120	12.888712000	10.1.1.25	10.1.1.5	SIP	517	Status: 100 Trying
121	12.988503000	10.1.1.25	10.1.1.16	SIP/SDF	869	Request: INVITE sip
122	12.988883000	10.1.1.25	10.1.1.5	SIP	533	Status: 180 Ringing
123	13.014938000	10.1.1.16	10.1.1.25	SIP	389	Status: 100 Trying
124	13.015931000	10.1.1.16	10.1.1.25	SIP	465	Status: 180 Ringing
125	13.016933000	10.1.1.25	10.1.1.5	SIP	533	Status: 180 Ringing
176	17.778122000	10.1.1.25	10.1.1.5	SIP	508	Status: 487 Request
181	17.907721000	10.1.1.16	10.1.1.25	SIP	440	Status: 487 Request



รูปที่ 6 รายละเอียดภายในแพ็กเก็ต INVITE

- ผลการทดลอง

.....

.....

.....

.....

.....

.....

.....

4.1.10 กดปุ่ม Clear ที่แถบ Filter เพื่อลบการกรองทั้งหมด

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

- ผลการทดลอง

.....

.....

.....

.....

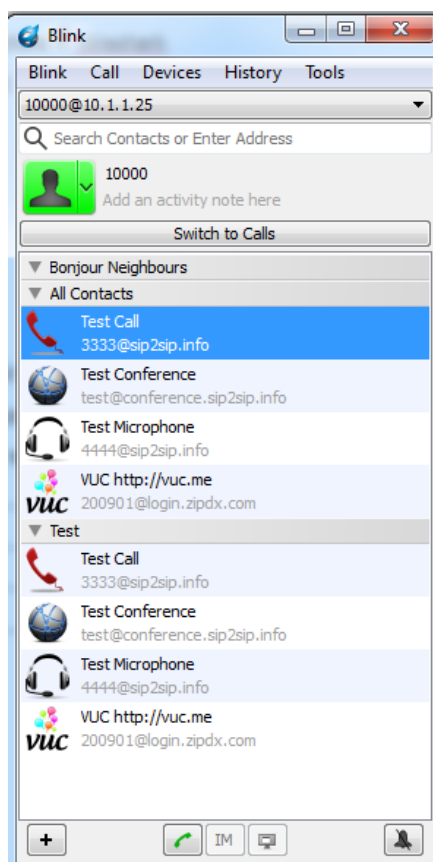
.....

.....

4.1.12 ปิดโปรแกรม X-lite

4.2 การเพิ่มความปลอดภัยในระบบ VoIP ด้วย TLS และ SRTP

4.2.1เปิดโปรแกรมซอฟต์แวร์โฟนBlinkซึ่งมีหมายเลขโทรศัพท์ คือ 10000 (หมายเลขนี้ถูกติดตั้งให้ใช้โพรโทคอลTLS และ SRTP ในการเชื่อมต่อการสนทนา)

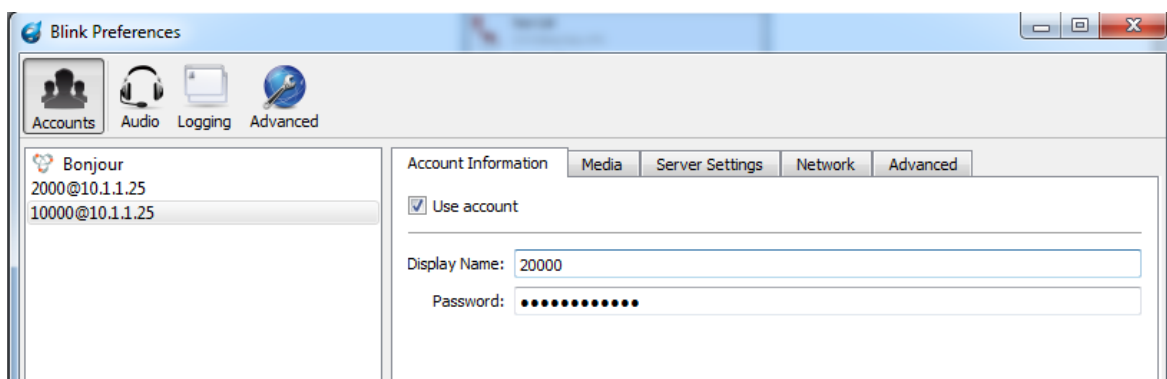


รูปที่ 7 Blink Softphone

4.2.2 เปิดโปรแกรมซอฟต์แวร์โฟนBlink ในเครื่องโน้ตบุ๊กอีกเครื่องแล้วทำการคอนฟิกค่าโทรศัพท์ เบอร์ 20000 ดังนี้

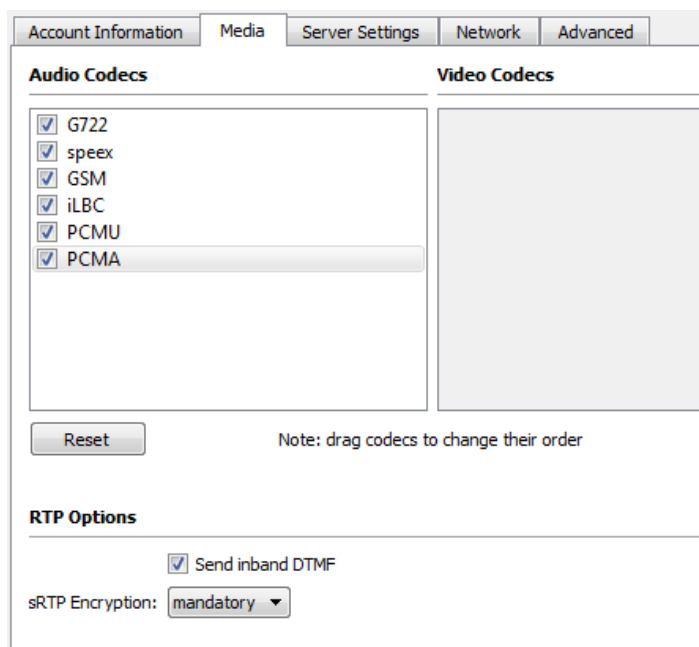
4.2.2.1 แท็บ Account Information

- Display Name: 20000
- Password: password20000



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

4.2.2.2 แท็บ Media เซตค่า sRTP Encryption: Mandatory



รูปที่ 9 การเซตค่า sRTP Encryption ใน Blink softphone

4.2.2.3 แท็บ Server Settings ใส่รายละเอียดของ IP-PBX

Outbound Proxy: 10.1.1.227

Port: 5061

Transport: TLS

Auth Username: 20000

The screenshot shows the Asterisk configuration interface for SIP Proxy settings. The 'Server Settings' tab is active. The 'SIP Proxy' section has the following configuration:

- Always use my proxy for outgoing sessions
- Outbound Proxy: 10.1.1.227
- Port: 5061
- Transport: TLS
- Auth Username: 20000

The 'MSRP Relay' section has the following configuration:

- Always use my relay for outgoing sessions
- MSRP Relay: Relay address taken from DNS
- Port: 2855
- Transport: TLS

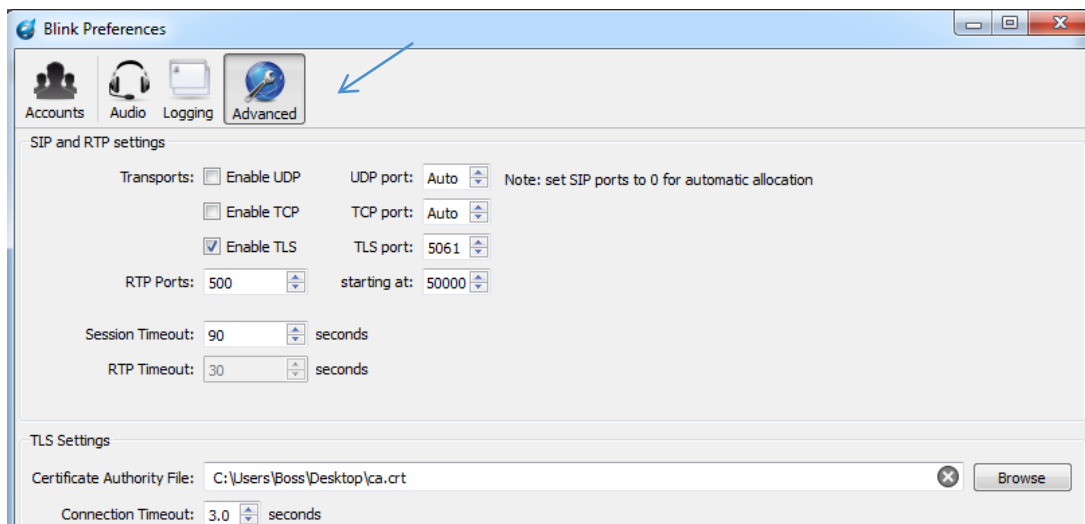
The 'Extra Server Settings' section has the following configuration:

- Voicemail URI: Discovered by subscribing to 10000@10.1.1.25
- XCAP Root URL: Taken from the DNS TXT record for xcap.10.1.1.25
- Server Tools URL: (empty)
- Conference Server: (empty)

รูปที่ 10 การเซตค่าเกี่ยวกับ IP – PBX

4.2.2.4 แถบเมนู เลือก Advanced

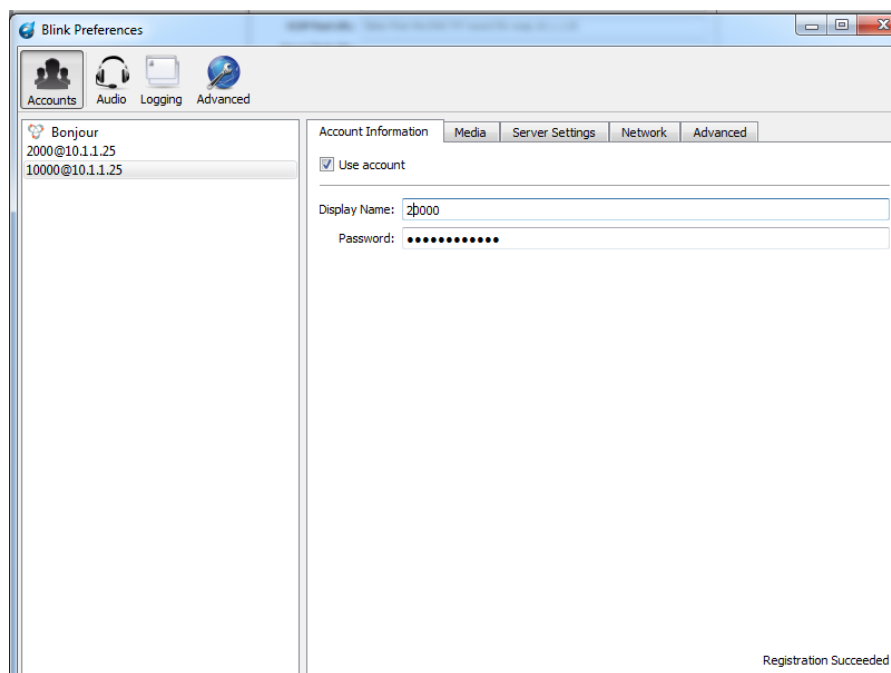
- Enable TLS
- เลือกไฟล์ ca.crt บนหน้าเดสก์ทอป ใส่เข้าไปใน Certificate Authority File



รูปที่ 11 การเซตค่า Enable TLS

4.2.2.5 ที่แถบเมนู เลือก Accounts-> Account Information

หากลงทะเบียนเรียบร้อยแล้ว 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

