ความปลอดภัยของการสื่อสารข้อมูลทางกว้างระบบดิจิตอล

เรือเอก ดนัย ปฏิยุทธ
กองวิชาวิศวกรรมศาสตร์ โรงเรียนนายเรือ

บทนำ

บทความเรื่องนี้เป็นการอธิบายถึงการป้องกันความปลอดภัยของการสื่อสารข้อมูลทางกว้างระบบดิจิตอล (Asynchronous Transfer Mode Security) โดยใส่ระบบความปลอดภัยไว้ที่ Control Plane โดยวิธีใหม่ที่ชื่อว่า Patiyoot's Mechanism

เนื้อเรื่อง

๑. ทั่วไป (Introduction)

ในโครงข่ายทางกว้าง (Broadband) นั้นจะใช้การสื่อสารทางกว้างระบบดิจิตอล (Asynchronous Transfer Mode) เป็นหลักซึ่งเป็นการสื่อสารที่รวมการส่ง เสียง รูปภาพ และอื่น ๆ ไว้ด้วยกันและทำการส่งในคราวเดียว ซึ่งการส่งไปยังจุดหมายปลายทางนั้นจะถูกแบ่งการส่งด้วยคุณภาพของการบริการ (Quality of Service) ซึ่งมีค่าบริการที่ต่างกันแล้วแต่องค์กรไหนจะเลือกใช้แบบใด ดังนั้นความจำเป็นในการรักษาความปลอดภัยในการส่งข้อมูลจึงมีความจำเป็นอย่างยิ่งยวดและขาดเสียมิได้ เพื่อมิให้บุคคลที่ไม่ได้สิทธิอันพึงมี กระทำการใด ๆ ที่มิชอบเพื่อให้ได้มาซึ่งสิทธินั้น ๆ

การบริการความปลอดภัย (Security Services) ด้านการสื่อสารข้อมูลทางกว้างระบบดิจิตอล (ATM) ของ Authentication, Confidentiality, Integrity, Access Control, Key Management, Availability หรือ Non-Repudiation นั้นสามารถให้บริการได้ที่ Plane ๓ แห่งด้วยกันคือ

๑. *User Plane*

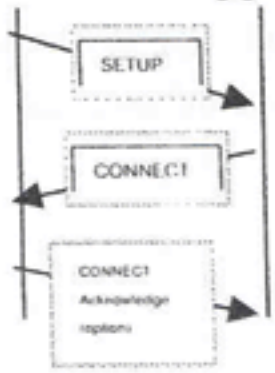
๒. *Control Plane*

๓. *Management Plane*

๒. ความปลอดภัยที่ชั้นควบคุม (Control Plane Security)

ที่ชั้นควบคุมนี้ สัญญาณควบคุม (Signaling Messages) โดยส่วนใหญ่จะมี ๒ สัญญาณด้วยกันคือ SETUP และ CONNECT และสัญญาณที่ ๓ (CONNECT ACKNOWLEDGEMENT) จะมีหรือไม่มีก็ได้ ดังแสดงในรูปที่ ๑ ซึ่งกระบวนการในรูปนี้จะได้มาซึ่ง Authentication ของสัญญาณควบคุมคือเป็นการบ่งบอกว่าผู้ส่งที่แท้จริงใช่บุคคลที่กล่าวอ้างหรือไม่

ผู้เรียกหรือผู้ส่ง (Calling Entity) ผู้ถูกเรียกหรือผู้รับ (Called Entity)



รูป ๑ กระบวนวิธี (Procedure) สำหรับ Authentication ของข้อความสัญญาณ (Signaling Message)

๒.๑ Patiyoot's Mechanism

ส่วนการจัดหาบริการความปลอดภัยสำหรับ Authenticationและ Key Exchange นั้น เราสามารถกระทำได้โดยการเพิ่ม IE เข้าไปอีก ๑๖ ตัวด้วยกันใน ข้อความ SETUP และ CONNECT โดยในแต่ละ IE จะมีข่าวสารหลายตัว ซึ่ง Authentication และ Key Exchange แสดงได้โดยในรูป ๒

$A \Rightarrow B\ Cert_A, S_{KSA}((E_{KPB}(A, N_A, T_A))$ (Message#1)

$B \Rightarrow A\ Cert_B, S_{KSB}(E_{KPA}(A, B, N_A, N_B, T_A, T_B, K_{AB}))$ (Message#2)

รูป ๒ การแลกเปลี่ยนข้อมูลระหว่างจุด A และ B เพื่อการให้บริการความปลอดภัยของการส่งข้อมูลสำหรับ Authentication และ Key Exchange โดยวิธี Patiyoot's Mechanism

โดย

A :	Identity of Calling Entity	B :	identity of Called entity
$Cert_A$:	A's public key certificate	$Cert_B$:	B's public key certificate
N_A :	A's nonce	N_B :	B's nonce
T_A :	Timestamp generated by A	T_B :	Timestamp generated by B
K_{SA} :	Secret key of A	K_{SB} :	Secret key of B
K_{PA} :	Public key of A	K_{PB} :	Public key of B
K_{AB}:	Session key		

$S_{KSA}(M)$: Message hashed and signed using A's secret key

$S_{KSB}(M)$: Message hashed and signed using B's secret key

$E_{KPA}(M)$: Message encrypted with A's public key

$E_{KPB}(M)$: Message encrypted with B's public key

รายละเอียดของ IE ที่เพิ่มเข้ามาอีก ๑๖ ตัวมีรายละเอียดการทำงานดังต่อไปนี้

๑. เมื่อ A ต้องการสื่อสารกับ B, A จะส่งข้อความ IE#13, IE#14 และ IE#1-IE#6 ในข้อความ SETUP, โดย Timestamp (T_A) และ Nonce (N_A) ที่ส่งไปใน IE#14 จะใช้ตรวจสอบในเวลาต่อมาว่าข้อความนั้น ๆ ที่ส่ง TA และ N_A มาด้วย ใหม่ (fresh) หรือไม่ และข้อความได้ถูกส่งถ่าย (relayed) มาหรือเปล่า

๒. เมื่อ B ได้รับข้อความที่ A ส่งมา, B จะทำการตรวจสอบ Certificate ว่าเป็นของ A จริงหรือไม่

๓. หลังจากนั้น B จึงนำ Public key ที่อยู่ใน Certificate มาใช้ตรวจสอบ การเป็นตัวตนที่แท้จริง (Authentication) ของ A

๔. หลังจาก B แน่ใจแล้วว่าผู้ที่ส่งข้อความมาคือ A, B จะส่งข้อความ IE#15, IE#16 และ IE#7-IE#12 ในข้อความ CONNECT เพื่อให้ A ตรวจสอบ การเป็นตัวตนที่แท้จริง (Authentication) ของ B, โดย Timestamp (T_B) และ Nonce (N_B) ที่ส่งไปใน IE#16 จะใช้ตรวจสอบในเวลาต่อมาว่าข้อความนั้น ๆ ที่ส่ง T_B และ N_B มาด้วย ใหม่ (Fresh) หรือไม่ และข้อความได้ถูกส่งถ่าย (Relayed) มาหรือเปล่า

๕. ถ้า A ตรวจสอบแล้วว่าB เป็นตัวตนที่แท้จริง A จะส่งข้อความ CONNECT Acknowledge และจะนำ Session key K_{AB} ไปใช้ในโอกาสต่อไป ถ้า A ตรวจสอบแล้วว่าB เป็นตัวตนที่ไม่แท้จริง, A จะส่งข้อความ RELEASE

โดยแสดงเป็นขั้นตอนได้คือ IE#1-IE#6 อยู่ในข้อความ SETUP

IE#1 : Calling Entity identifier

IE#2 : Type of confidentiality, Integrity, Key Exchange

IE#3 : Function type: real time, non real time

IE#4 : Confidentiality parameter: list of algorithm

IE#5 : Integrity parameter: list of algorithm

IE#6 : Key Exchange parameter: list of algorithm

โดย Calling Entity Identifier ใน IE#1 คือการแสดงตัวตนของผู้ส่งและจะถูกเก็บไว้ที่ผู้รับตลอดเวลาการติดต่อสื่อสาร ผู้ส่งจะถามผู้รับในข้อความ IE#2 ว่าต้องการความปลอดภัยรุ่นไหนจากตัวเลือกคือ Confidentiality, Integrity หรือ Key Exchange หรือทุกตัว ผู้ส่งจะตอบมาโดยข้อความ IE#8, ใน IE#3 ผู้ส่งจะถามผู้รับว่าต้องการฟังก์ชั่นแบบ Real Time หรือ non real time โดยผู้รับจะตอบมาใน IE#9

ใน IE#4 ผู้ส่งจะให้ผู้รับเลือก ตัวแปร (Parameter) ของ Confidentiality โดยผู้รับจะตอบมาใน IE#10 ใน IE#5 ผู้ส่งจะให้ผู้รับเลือก ตัวแปร (Parameter) ของ Integrity โดยผู้รับจะตอบมาใน IE#11 ใน IE#6 ผู้ส่งจะให้ผู้รับเลือก ตัวแปร (Parameter) ของ Key Exchange โดยผู้รับจะตอบมาใน IE#12

IE#7-IE#12 อยู่ในข้อความ CONNECT

IE#7 : Called Entity identifier

IE#8 : Chosen Type of Confidentiality, Integrity, Key Exchange

IE#9 : Chosen Function Type

IE#10 : Chosen Confidentiality parameter: chosen algorithm

IE#11 : Chosen Integrity parameter: chosen algorithm

IE#12 : Chosen key Exchange: chosen algorithm

ข้อความ IE#13 และ IE#14 นั้นอยู่ในข้อความ SETUP เพื่อการทดสอบ Authentication และ Key Exchange โดยเมื่อ B รับข้อความ, B ก็จะตรวจสอบว่าตัวเองเป็นผู้ที่ A ติดต่อด้วยหรือไม่และ A เป็นผู้ส่งตัวจริงหรือไม่ หลังจากนั้น B จะทำการดึงเอาข้อมูลออกจาก $Cert_A$ เพื่อพิสูจน์ว่าข้อมูลนั้นสามารถใช้งานได้ ตรวจสอบ Signature ของ A เพื่อ Integrity

IE#13 : $Cert_A$

IE#14 : $S_{KSA}(E_{KPB}(A, N_A, T_A)$

ข้อความ IE#15 และ IE#16 นั้นอยู่ในข้อความ CONNECT เพื่อการทดสอบ Authentication และ Key Exchange โดยเมื่อ A รับข้อความ, A ก็จะตรวจสอบว่าตัวเองเป็นผู้ที่ B ติดต่อด้วยหรือไม่และ B เป็นผู้ส่งตัวจริงหรือไม่ หลังจากนั้น A จะทำการดึงเอาข้อมูลออกจาก $Cert_B$ เพื่อพิสูจน์ว่าข้อมูลนั้นสามารถใช้งานได้ ตรวจสอบ Signature ของ B เพื่อ Integrity

IE#15 : CertB

IE#16 : $S_{KSB}(E_{KPA}((A, B, N_A, N_B, T_A, T_B, K_{AB})$

สรุป

เอกสารเรื่องนี้เป็นการอธิบายถึงการป้องกันความปลอดภัยของการสื่อสารข้อมูลทางกว้างระบบดิจิตอล (Asynchronous Transfer Mode Security) แบบ Authentication และ Key Exchange โดยใส่ระบบความปลอดภัยไว้ที่ Control Plane โดยการเพิ่มข้อความ IE#1 ถึง IE#16 เข้าไปที่ข้อความสัญญาณ

อ้างอิง

๑. M. Laurent, *"Securing communications over ATM"*, Proceeding of IFIPSEC 13 th International Security Conference, 1997.

๒. M. Laurent, *"ATM Security State of the Art"*, Proceeding of ATM development, March 1998.

๓. R.H. Deng et al, *"Securing Data transfer in Asynchronous Mode Networks"*, Proceeding GLOBECOM'95, November 13-17 1995, pp.1198-1203.

๔. L. Hansen, *"The impact of ATM on Security in the Data Network"*, Compsec international proceeding, 1995, pp.318-324.

๕. S.C. Chuang, *"Securing ATM networks"*, 3th ACM Conference on Computer Communication Security, 1996.