5907101012 มุขยา วงศ์ดาราพานิช

**Wireless Security on Wireless LAN**

**Wireless Security**

คงต้องเกริ่นพื้นฐานของหัวข้อนี้ก่อน โดยการพูดถึง Security ใน Wireless network นั้นเราจะพูดถึงการไม่ได้รับอนุญาติในการเข้าถึง หรือสร้างความเสียหาย ให้กับคอมพิวเตอร์หรือData โดยใช้ wireless network นั่นเอง

พูดถึงเนื้อหาคร่าวๆของหัวข้อนี้ เราคงจะต้องพูดถึงสิ่งที่เราเห็นได้บ่อยในชีวิตประจำวันเช่น WPA(Wi-Fi Protected Access) หรือเก่ากว่านั้น WEP (Wired Equivalent) ซึ่งตัว WEP นั้นเป็น wireless security รูปแบบเก่าซึ่งปัจจุบันถูกแทนที่ด้วย WPA/WPA2 หมดแล้ว โดยปกติทั่วไปตอนนี้ตามบ้านหรือครัวเรือนทั่วไปจะใช้ WPA เนื่องจากบางอุปกรณ์ยังไม่รอบรับ WPA2 โดยทั้ง WPA และ WPA2 ก็คือการ encryption device นั่นเอง

โดยทั่วไป Laptop จะมีอุปกรณ์ที่เรียกว่า wireless cards ติดตั้งไว้อยู่แล้ว เพื่อใช้ในการเข้าถึง network ในขณะที่มือถือก็มีเช่นกัน ซึ่ง attacker หรือ hacker นั้นได้ค้นพบว่าจริงๆแล้ว wireless networkนั้นง่ายต่อการโจมตีอย่างมาก ยิ่งไปกว่านั้นสามารถทำการโจมตี wireless network แล้วลามไปถึง wired network ได้อีกด้วย เพราะฉะนั้นเป็นเรื่องที่ต้องตื่นตัวอย่างมากในการทำงานระดับ enterprises เกี่ยวกับการเข้าถึงและ policies ของการเข้าถึงที่ไม่ได้รับอนุญาติในwireless network

ในหัวข้อถัดๆไปจะมีการพูดถึงรูปแบบต่างๆของภัยอันตรายที่สามารถเกิดขึ้นได้ในอุปกรณ์ไร้สาย

ยกตัวอย่างให้เข้าใจง่ายที่สุด เนื่องจาก wireless security ก็เป็นเพียงมุมนึงของ computer security และมีระบบการป้องกันที่ค่อนข้างอ่อนแอต่อการโจมตี

นึกภาพตัวอย่างในบริษัทแห่งนึงมีพนักงาน เอาอุปกรณ์ wireless routerเข้ามาเสียบเข้ากับ switch ที่ใช้ในบริษัท ผลที่ตามมาคือระบบ network ทั้งหมดอาจถูกเปิดเผยให้กับใครก็ตามที่อยู่ในระยะการสื่อสารของ wireless router ตัวนั้น หรือแม้แต่พนักงานเพิ่ม wireless interface ไปที่คอมพิวเตอร์โดยใช้สาย USB port อาจก่อให้เกิดการคุกคามได้เช่นกัน เพราะมันถือเป็นการอนุญาติการเข้าถึง ถึงแม้บางหัวข้ออาจแก้ได้ในเบื่องต้น ยกตัวอย่างข้อแรกที่มีพนักงานนำ wireless routerเข้ามาต่อ อาจแก้ได้ด้วยการทำ VLAN หรือ limit การเข้าถึง network access แต่นั่นหมายถึงการที่เราจะต้องทำแบบนั้นกับอุปกรณ์ switch ทุกตัวอย่างแมนวล

เนื่องจากในปัจจุบัน ระบบเครือข่ายไร้สายเริ่มเป็นที่แพร่หลายมากขึ้น แน่นอนว่าการพยายามเข้าถึงข้อมูลโดยไม่ได้ระบอนุญาติ ผ่านระบบเครือข่ายไร้สายก็จะมีมากขึ้นอย่างไม่ต้องสงสัย ความเสี่ยงในการใช้ระบบเครือข่ายไร้สายก็จะมีมากขึ้นด้วยนั่นเอง รวมไปถึงวิธีการป้องกันที่ต้องมีความซับซ้อนมากยิ่งขึ้นอีกด้วย

เราจะมาพูดถึงหัวข้อการโจมตีต่างๆบน Wireless network เพื่อให้ง่ายต่อการเข้าใจ

**Rogue APs**

พูดง่ายๆคือ access point ปลอมนั่นแหละ โดยมีจุดเด่นดังนี้

Rogue APs ไม่ใช่ส่วนนึงของ network infrastructure หรือพูดอีกนัยนึงคือเกิดขึ้นมาลอยๆ โดยมีการแอบอ้างตัวเองขึ้นมานั่นเอง

เมื่อมีการเชื่อมต่อเข้าไปที่ตัว Rogue APs จะทำให้ตัวคนที่เชื่อมต่อเข้าไปกลายเป็น rogue client และนั่นทำให้คนที่เชื่อมต่อเข้าไปสามารถโดนการ bypass ผ่านพวก security policy ได้

รูปแบบข้างต้นเป็นเพียงตัวอย่างแรก ยังจะมีแนวทางอย่างอื่นอีกมากมายในการคุกคามและโจมตี

โดยจะมีรูปแบบทั่วๆไปคือการเข้าถึงโดยไม่ได้รับอนุญาติ

**Ad Hoc Networks**

การคุยกันระหว่าง 2 node ก็มีความเสี่ยงจะเกิดการโจมตีได้เช่นกัน โดย

• Attacker สามารถสร้าง ad hoc network ที่น่าเชื่อถือขึ้นมาเพื่อทำการขโมยข้อมูล หรือ logs จากผู้ใช้

• ใช้ ad hoc networks ในการเข้าถึง Wired network

• bypass นโยบายด้าน security

**Client Misassociation**

เมื่อ client เชื่อมต่อเข้าไปใน access point ตัวอุปกรณ์ที่ใช้เชื่อมต่อโดยส่วนมากจะจดจำ SSID หรือให้เข้าใจง่ายๆก็คือจดจำชื่อของ network ที่เชื่อมต่อเข้าไป เพื่อที่ว่าถ้าคราวหน้าเห็น SSID นี้ก็จะทำการเชื่อมต่ออีกครั้งโดยอัตโนมัติ

Attacker สามารถทำการมอง SSID ที่อุปกรณ์ของเราเชื่อมต่ออยู่ จากนั้นใช้ข้อมูลตรงนี้ในการสร้างอุปกรณ์บางอย่างขึ้นมาเพื่อกระจายสัญญาณที่ใช้ SSID แบบเดียวกันที่เป็น wireless station เมื่ออุปกรณ์ของเราเห็น SSID ที่เคยเชื่อมต่อจากการปลอมตัวของ Attacker อุปกรณ์ของเราก็จะเชื่อมต่อเองโดยอัตโนมัติ ทำให้ Attacker สามารถเข้ามาขโมยข้อมูลในอุปกรณ์ที่เชื่อมต่อได้นั่นเอง

**Identity theft (MAC Spoofing)**

Identity theft หรือ MAC Spoofing จะเกิดขึ้นเมื่อ hacker หรือ attacker มีการดักจับ network traffic แล้วรู้ MAC Address ของคอมพิวเตอร์ที่มีสิทธิ์ในการเข้าถึง network

เพราะโดยปกติส่วนใหญ่ Access point จะมีสิ่งที่เรียกว่า MAC Fillering ซึ่งเป็นการรับเฉพาะ MAC Addressบางตัวเท่านั้น ที่ได้ทำการลงทะเบียนไว้ล่วงหน้าให้สามารถเข้าใช้ network ได้

โดยซอฟแวร์ที่ใช้ในการ sniffing หรือใช้ในการตรวจจับ packet หรือรับ packet ผ่าน data streams นั่นมีอยู่ ร่วมกับการทำ spoofing แล้วนั้น จึงเป็นการเข้าถึง network โดยปลอมเป็นอุปกรณ์ได้นั่นเอง

**Type of Attacks**

Reconnaissance attacks : attacker พยายามจะเพิ่มสิทธิ์ในการเข้าถึงข้อมูลภายในเน็ตเวิร์ค

Access attacks : attacker พยายามจะเพิ่มสิทธิ์ในการเข้าถึงข้อมูล รวมไปถึงอุปกรณ์ หรือเน็ตเวิร์ค

Denial-of-service (DoS) attacks : attacker พยายามที่จะโจมตีเพื่อทำให้ผู้ใช้ไม่สามารถใช้งาน service ใดๆ ที่ตัวผู้ใช้ต้องการเข้าถึง เช่นการเข้าถึงเว็บไซต์ต่างๆ

พูดถึงรูปแบบการโจมตีมาเยอะพอสมควร เรามาพูดเรื่องรูปแบบการป้องกันบ้างดีกว่า

**Security measures**

ตามชื่อก็คือมาตรการด้านความปลอดภัยนั่นเอง ซึ่งมีหลากหลายมากใน wireless network

**SSID hiding**

ก่อนหน้านี้มีการพูดถึงเรื่องการปลอม SSID จาก attackerมาแล้ว นี่เป็นอีกหนึ่งวิธีในการป้องกัน ถึงจะไม่ค่อยมีผลมากนัก โดยการซ่อน SSID บนอุปกรณ์ของตัวเองซะโดยการ set SSID ไว้ที่ null ทุกครั้งที่มีการส่ง packet แต่ไม่ใช่วิธีที่ยั่งยืนนักแต่สามารถทำได้ง่าย

**MAC ID filtering**

เป็นอีกหนึ่งวิธีที่ไม่ยากต่อการทำคือการ allow access ที่ได้รับอนุญาติโดยทำการ assign ไว้ล่วงหน้าเท่านั้น และใช้ MAC addresses เป็นตัว allow access โดยอุปกรณ์ Access point บางตัวจะมีระบบ MAC ID Filtering อยู่ในตัวอยู่แล้ว

แต่นั่นก็ไม่สามารถปกป้องข้อบกพร่องทั้งหมดได้เพราะฝั่ง attacker เอง ก็สามารถทำการปลอม MAC Address ได้เช่นกัน (MAC spoofing)

**IEEE 802.1X**

IEEE 802.1X เป็นหนึ่งในมาตรฐาน IEEE Standard authentication ที่อุปกรณ์ส่วนใหญ่ที่สามารถเข้าถึง wireless LAN จะต้องมี

**Pre-Shared Key**

อธิบายอย่างง่ายคือมีการขออนุญาติกันก่อนที่จะมีการส่งข้อมูลหากันนั่นเอง รวมไปถึงเป็นหนึ่งในขั้นตอนของ WEP เนื่องจาก WEP ก็ใช้ key ในการติดต่อสื่อสารเหมือนกัน โดยมีขั้นตอนคร่าวๆดังนี้

1. ผู้ส่งขอ authentication request
2. ฝั่ง AP ส่ง authentication response ซึ่งพ่วง clear text ที่สามารถให้ฝั่งผู้ส่งใส่ข้อมูลลงมาแล้วส่งมาได้
3. ผู้ส่งใส่ข้อมูลที่ทำการ encryp แล้วด้วย WEP(ตัวอย่าง) แล้วส่งไปหา AP
4. AP ทำการเปรียบเทียบข้อมูลที่ได้รับมา กับข้อมูลที่มีอยู่ทางฝั่งผู้ส่ง ถ้าทั้งสองฝั่งเหมือนกัน ถือว่าการสื่อสารเสร็จสิ้น

**Wired Equivalent Privacy (WEP)**

เป็นหนึ่งในรูปแบบมาตรฐานการ encryption บน wireless โดยใช้รุปแบบที่เป็น key ในการ encrypt ข้อมูล หลักการและตัวอย่างดังต่อไปนี้

Standard 64-bit WEP

จะพูดถึงตัว WEP โดยใช้การ encryption ด้วย key ขนาด 64 bit โดยจะแบ่งเป็นสองส่วน ส่วนที่เป็น key กับส่วนที่เป็น initialization vector(IV)

แบ่งเป็น key 40 bit (เรียกอีกอย่างว่า WEP-40) และ IV 24 bit

จากนั้นนำทั้งสองส่วนทำการ XOR กันก็จะได้ส่วนที่เป็น Cipher text ส่งออกไป

แต่วิธีนี้เป็นวิธีที่เก่า รวมไปถึงขั้นตอนค่อนข้างง่ายต่อการ crack เพราะใช้อัลกอริทึ่มง่ายๆอย่างการ XOR จึงถูกแทนที่ด้วยระบบใหม่ๆที่ตามมาภายหลัง

**WPA**

ถูกใช้อย่างแพร่หลายหลังจาก WEPและเข้ามาแทนที่ WEP ในที่สุด ใช้หลักการ Temporal Key Integrity Procol (TKIP) ในการเปลี่ยนแปลง Keys ในทุกๆ packet

รวมไปถึง support advanced encryption standard อีกด้วย

WPA Modes

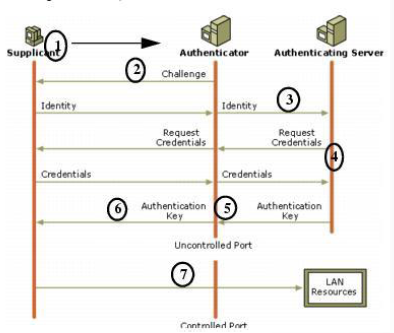
บน WPA นั้น มีการ authentication อยู่หลักๆ 2 modes

• Enterprise mode: ใน Enterprise mode นั้น WPA จะต้องมี authentication server เพื่อใช้ในการทำ authentication รวมไปถึงเป็นส่วนประกอบในการใช้ key และการทำ TKIP

• Personal mode: ใน Personal mode นั้น WPA จะใช้สิ่งที่เรียกว่า pre-shared keys ในการสื่อสารแทน ซึ่งทำให้รูปแบบการ encryp ข้อมูลอ่อนแอลงนั่นเอง แต่ก็เพียงพอสำหรับการใช้ในครัวเรือน เพราะง่ายต่อการติดตั้งและจัดการ

หลักการของ WPA ค่อนข้างมีความใกล้เคียงกับ WEP เนื่องจากมีการขอ request คล้ายๆกัน เพียงแต่ WPA จะใช้สิ่งที่เรียกว่า EAP ในการติดต่อสื่อสารระหว่างกันใน Enterprise Mode เช่นมีการข้อ EAP-Start message การใช้ EAP-request identity message, response packet

เพื่อให้ทาง Authentication Server อนุญาติให้เข้าใช้ port ที่ซึ่งได้รับอนุญาติจาก EAP ดังรูป



WPAv2

ตัว WPAv2 นั้นจะใช้มาตรฐานใหม่ เรียกว่า 802.11i (แต่ก็ต้องการอุปกรณ์ชนิดใหม่ด้วยเช่นกัน ไม่อย่างนั้นต้องทำการ update firmware บนอุปกรณ์เครื่องเก่า)

โดยหลักๆมีฟังชั่นเพิ่มเติมคือ AES-CCMP algorithm โดยยังมี EAP authentication เช่นเดิม

AES-CCMP algorithm

Counter Mode Cipher Block Chaining Message Authentication Code Protocol (Counter Mode CBC-MAC Protocol) หรือ CCM mode Protocol (CCMP) (ปล.ตัวย่อมากมายเหลือเกิน)

คือ encryption protocol ดีไซน์ใหม่ที่เพิ่มเข้ามาใน IEEE 802.11i โดย CCMP จะทำการเพิ่มการทำ encryption บน data ซึ่งเป็นหนึ่งในมาตรฐาน encryption ขั้นสูง โดยมี service ที่เพิ่มขึ้นมาดังนี้

• Data confidentiality : การรับรองการเข้าถึงข้อมูลโดยเฉพาะผู้ที่ได้รับอนุญาติให้เข้าถึง data เท่านั้น

• Authentication : มีการทำ proof user ที่ทำการเข้าถึง

• Access control : เชื่อมต่อการจัดการกับ layer management

อีกทั้ง CCMP ยังใช้ key ขนาด 128-bit key นั่นหมายถึงการป้องกันการโจมตีจากการทำ brute force attack ได้ถึง 2^64 อีกด้วย