Netzsicherheit – Architekturen und Protokolle
Infrastruktursicherheit

Wireless LAN

Wireless LAN (WLAN) IEEE 802.11

- private Nutzung
- Nutzung in der Internet-Infrastruktur (WLAN-Hotspots)
- Zugangskontrolle besonders wichtig
  - → kein physischer Kontakt zur Kommunikation notwendig

- WEP
  - Sicherheitsmechanismen für LAN-äquivalente Sicherheit
- WPA, WPA2, 802.11i
  - Verbesserung der Sicherheit und Behebung der Probleme von WEP
- EAP-TLS, PEAP, EAP-TTLS
  - Beidseitige Authentifizierung mit EAP
- 802.11w
  - Sicherung von Management Rahmen

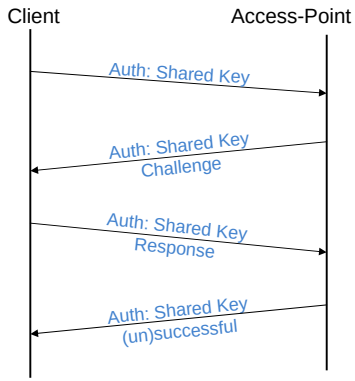
Wired Equivalent Privacy

Wired Equivalent Privacy (WEP)

- Klassen von Authentifizierungsdiensten
  - *Open System:* keine Authentifizierung, nur Handshake
  - *Shared Key:* alle Benutzer verwenden gleichen Schlüssel
- Schlüssel
  - Verschlüsselung mit Stromchiffre RC4
  - Statischer 40 Bit Schlüssel, mit zufällig gewähltem 24 Bit `IV` als Eingabe für Schlüsselerzeugung
  - Key-Management und Erneuerung aufwendig
- Probleme
  - kurzer und statischer Schlüssel
  - kurzer `IV`, Rollover und erneute Nutzung möglich
  - Tools wie *AirSnort* und *WEPcrack* knacken WEP-Schlüssel

Authentizierung bei WEP

- Klassisches Challenge-Response-Verfahren
- Challenge wird mit Schlüssel via WEP verschlüsselt



Angriff auf Authentifikation

1. Client generiert `IV1`, berechnet Schlüsselzeichen

`Secret Key` (40 Bit) + `IV1` (24 Bit) → RC4 → `Key1`

2. Client berechnet

`Response1=Challenge1 XOR Key1`

3. Angreifer erlauscht

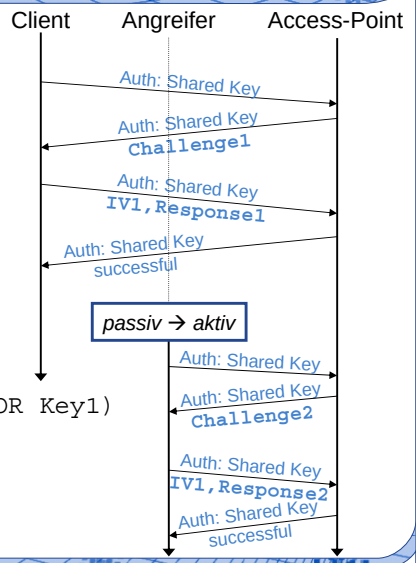
`Challenge1, IV1, Response1`

4. Angreifer berechnet

`Challenge1 XOR Response1`
`= Challenge1 XOR (Challenge1 XOR Key1)`
`= Key1`

→ `IV1` und `Key1` sind gültige Kombination

`Response2 =Challenge2 XOR Key1`



WEP2

- Vielzahl von Angriffen gegen WEP
  - `RC4` als Pseudozufallszahlengenerator mit schwachen `IVs` ungeeignet → viele schwache Schlüssel
  - Kontrollnachrichten nicht authentifiziert → DoS möglich
  - Known-Plaintext-Angriffe möglich (ARP, IP- und TCP-Header)
- Verbesserungen in WEP2
  - Verlängerung des Schlüssels
    - WEP 40 (+24=64) Bit, WEP2 104 (+24=128) Bit
  - Nutzung von 802.1x zur Authentizierung
  - Austausch von Session-Keys via 802.1x-Key-Nachrichten
  - Kerberos-5-Support ist verpflichtend
- Verbleibende Probleme
  - Kontrollnachrichten immer noch nicht authentifiziert
  - weiterhin Verwendung von `RC4`

  → WEP2 ebenfalls schon gebrochen, da Probleme mit `RC4` und schwachen `IVs` weiterhin bestehen

WPA / WPA2 / 802.11i

- Lang andauerndes Problem
  - Standardisierungsprozess von 802.11i sehr langwierig
  - Kernfunktionalität fix und WEP inzwischen vollständig gebrochen
- Lösung
  - WiFi-Allianz definiert WiFi Protected Access (WPA) Profil
  - Nutzung neuer, verbesserter Algorithmen von 802.11i
    - Verbesserte Verschlüsselung: Temporal Key Integrity Protocol (TKIP)
    - Verbesserter Authentizitätsschutz: Michael

  → anwendbar auf herkömmlicher WEP-Hardware!
- Inzwischen
  - 802.11i verabschiedet und deutlich sicherer als WPA und WEP
    - TU Darmstadt: *Breaking 104 bit WEP in less than 60 seconds*, 2007
  - WPA2 ist Profil für volle Sicherheit (z.B. Nutzung von AES-CCM verpflichtend)

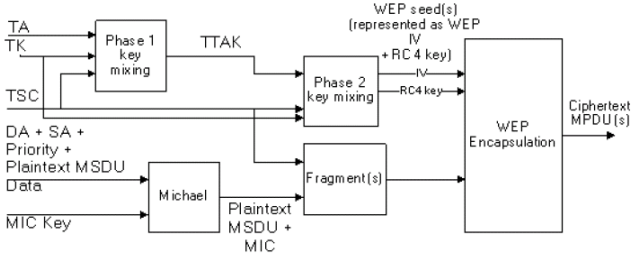
802.11i – Überblick

- Authentifizierung: Handshake über EAPoL/802.1x mit beidseitiger Authentifikation (z.B. EAP-TLS)
- Neues Modell zum Schlüsselmanagement
  1. **Client und AS** erzeugen Hauptschlüssel (Master Key)
  2. Individueller Hauptschlüssel (Pairwise Master Key, PMK) für **Client** und **AP**. Transport zum **AP** via RADIUS
  3. **Client, AP**: 4-teiliger EAPoL-Key-Austausch erzeugt aus PMK temporären Schlüssel (Pairwise Transient Key, PTK)
  4. Aufspaltung des PTK in Unterschlüssel
     - Data Encryption Key, Data MIC Key
     - EAPoL Encryption Key
  5. **AP** sendet Client einen mit EAPoL Encryption Key verschlüsselten temporären Gruppenschlüssel (*Group Transient Key, GTK*)
     - Group Encryption Key
     - Group Integrity Key

Neue Verfahren in 802.11i / WPA

802.11i Draft 3 / WPA

- Temporal Key Integrity Protocol
  - verwendet MAC-Adresse und zusätzlichen Schlüssel um per Mixing weiteren Zufall in RC4-Eingabe zu Erzeugen
- Michael
  - sehr einfaches Verfahren zur Integritätssicherung von Daten
  - kann ohne Änderungen auf WEP-Hardware laufen

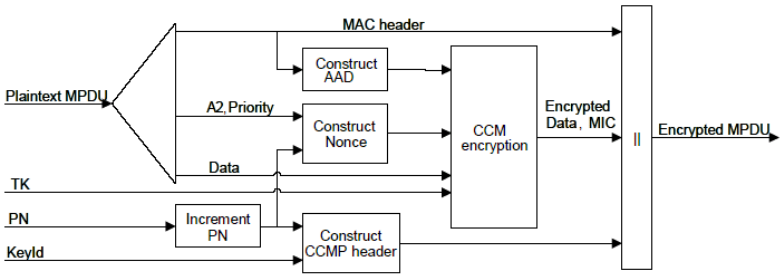


TA	Transmitter Address	TK	Temporal Key (wird aus PTK gewonnen)
TSC	TKIP Sequence Counter	TTAK	TKIP-mixed Transmit Address and Key

Neue Verfahren in 802.11i / WPA2

802.11i final / WPA2

- zusätzlich AES-CCM
- Verschlüsselung und Authentifizierung mit AES



PN	Packet Number	TK	Temporal Key (wird aus PTK gewonnen)
A2	Adresse 2	AAD	Additional Authentication Data bestimmte Felder im MAC-Header (Adressen, Flags, QoS, …)

Überblick über die Modi

	WPA PSK Modus	WPA (Enterprise) Modus	WPA2 Personal Mode	WPA2 Enterprise Mode
Optionale Algorithmen	AES-CCM	AES-CCM	TKIP + Michael	TKIP + Michael
Verpflichtende Algorithmen	TKIP + Michael	TKIP + Michael	AES-CCM	AES-CCM
Authentifikation	Passwort	802.1x	Passwort	802.1x

Neue Anforderungen an EAP/802.1x bei WLAN

Probleme von EAPoL/802.1x bei Nutzung in WLAN

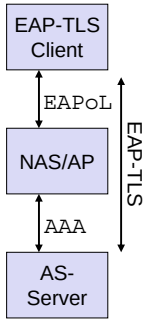
- Passive Angriffe einfacher möglich
  - Identitäten beim initialen Austausch können mitgehört werden
- Aktive Angriffe einfach möglich
  - Man-in-the-Middle-Angriff während Authentifikation, da Server nicht authentifiziert wird
  - Spoofen von Frames möglich, z.B. `End-of-Session` bei EAPoL
  - `EAP-Success/Failure`-Nachrichten ungeschützt
- daher
  - → Authentifizierung und Verschlüsselung von EAP notwendig
  - → Schlüsselmaterial für Authentifizierung/Verschlüsselung der Nutzdaten auf Link-Layer notwendig
  - häufiges Wechseln von NASen führt zu häufigem Authentifizieren
    - ➔ Mechanismus für schnelle Re-Authentizierung notwendig

EAP-Modul EAP-TLS

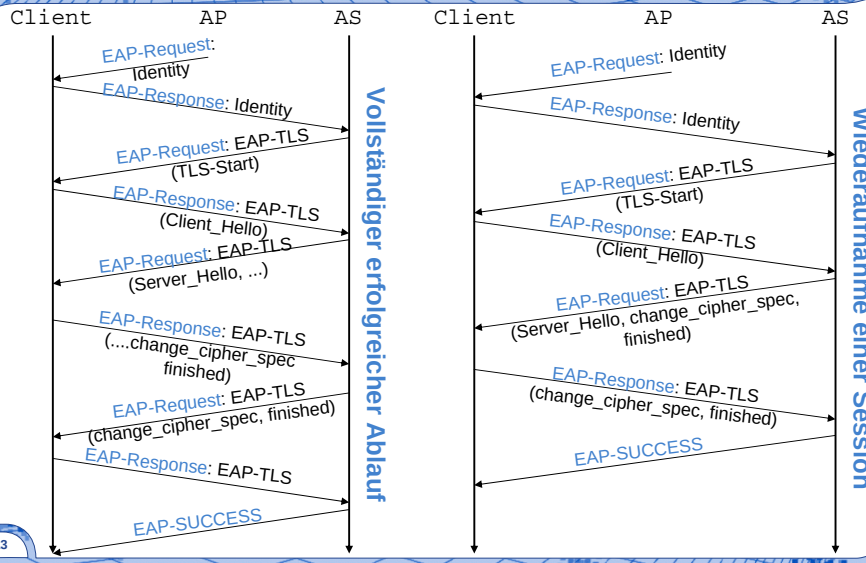
EAP-TLS

- Authentifizierung *beider* Kommunikationspartner
- Aushandlung einer Cipher-Suite

- Vorteile
  - Nutzung eines bewährten und geprüften Protokolls
  - Wiederaufnahme einer Session möglich
- Nachteile
  - Fragmentierung notwendig, falls TLS-Records zu lang
  - Authentifizierung des Clients über Zertifikate
  - Identitäten werden unverschlüsselt übertragen
  - Validierung des Serverzertifikates u.U. nicht möglich



EAP-TLS: Beispiel-Abläufe



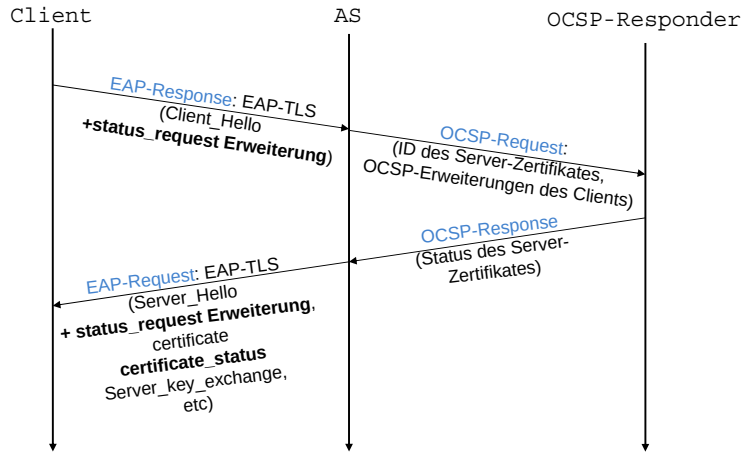
OCSP via TLS

Problem: Clients im Fall von 802.1x haben keine IP-Konnektivität
→ Statusüberprüfung für Serverzertifikate nicht möglich

Transport Layer Security Extensions

- Client kann vom Server OCSP-Bestätigung verlangen
- Client sendet erweitertes `Client_Hello` mit Erweiterung `status_request` mit akzeptablen OCSP-Respondern
- Wenn Server Erweiterung unterstützt
  - Weiterleitung der OCSP-Anfrage an OCSP-Responder mit vom Client mitgeschickten OCSP-Erweiterungen (z.B. Nonce)
  - Antworten mit `Server_Hello`-Nachricht mit Erweiterung `status_request` als Indikation dafür, dass Erweiterung bekannt
  - Senden der Antwort des OCSP-Responders (`Certificate_Status`)

Ablauf OCSP via TLS

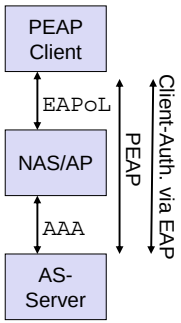


EAP-Modul: PEAP

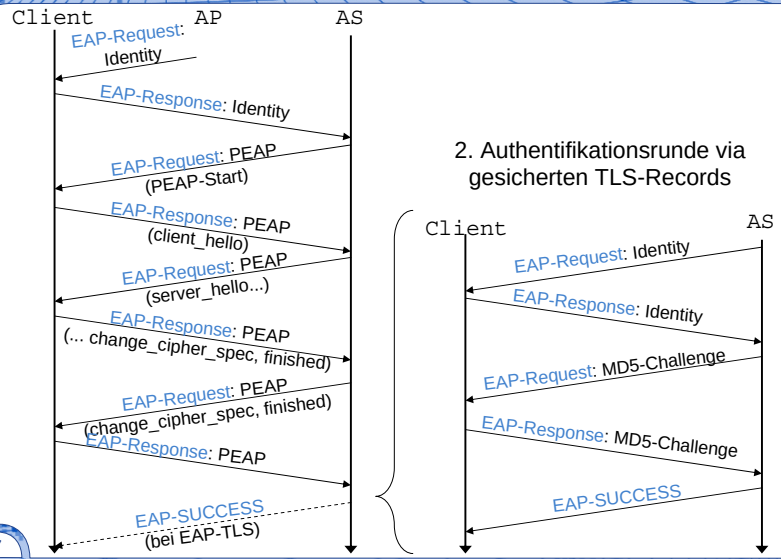
Protected EAP (PEAP)

- adressiert Probleme von EAP-TLS
- besteht aus 2 Phasen
  - *Phase 1*: Aufbau TLS-Verbindung (Client anonym)
  - *Phase 2*: geschützte Authentifizierung mit EAP
- Wiederaufnahme von Session ohne Phase 2

- Nachteile von PEAP
  - keine Aushandlung von Parametern für Sicherungsschicht
  - Client kann u.U. Server-Zertifikat nicht validieren
  - Umkopieren von `AS` Daten von EAP nach `AAA` bei Roaming



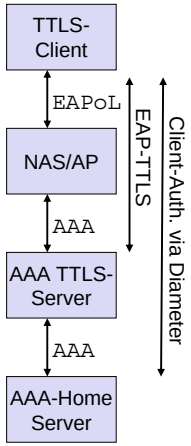
PEAP: Beispielablauf



EAP-Modul: TTLS

EAP Tunneled TLS Authentication Protocol

- 2 Phasen, gleiche Motivation wie PEAP, aber weitergehend
- in Phase 2 auch nicht-EAP-Mechanismen von PPP (z.B. CHAP)
- Unterschiede zu PEAP
  - Authentifizierung des Clients syntaktisch in Form von Diameter-PDUs
    - somit einfaches Weiterleiten der Authentifikationsdaten bei Roaming (kein Umsetzen von EAP nach Diameter)
  - Aushandlung von Algorithmen zur Sicherungsschicht zwischen `Client` und `AP/NAS`
  - Erzeugung und Verteilung von Schlüsselmaterial zur Sicherung des Link-Layers zwischen Client und `NAS/AP`



Andere Möglichkeiten

LEAP
- Cisco Light EAP
- unsicher
  - Passwörter nur mittels MS-CHAP geschützt
  - schwache Passwörter können gefunden werden (http://asleap.sourceforge.net)

EAP-FAST
- Nachfolger von LEAP: soll einfach wie LEAP und sicher wie PEAP sein
- basiert auf 2-Phasen-Ansatz
  - zuerst sicheren Tunnel aufbauen
  - dann MS-CHAP oder ähnliches für Passwortüberprüfung

EAP-SIM
- EAP mit GSM-Authentifizierung (SIM-Karte)

EAP-AKA
- EAP mit UMTS-Authentifizierung

EAP-IKEv2
- EAP mit IKEv2-Authentifizierung (Password, Preshared Key, Zertifikate, …)

Netzsicherheit – Architekturen und Protokolle
Infrastruktursicherheit

Protected Management Frames

IEEE 802.11w Protected Management Frames

- Problem
  - Bisher nur Rahmen mit Nutzdaten geschützt
  - Management-Rahmen ungeschützt
- Angriffe
  - DoS-Angriffe gegen Clients
    - z.B. Deauthentication-Flooding
  - neu aufkommende Funktionalität transportiert sensitive Daten in Management Frames
    - Fast Handoff, Radio Ressource Management, Wireless Network Management, …

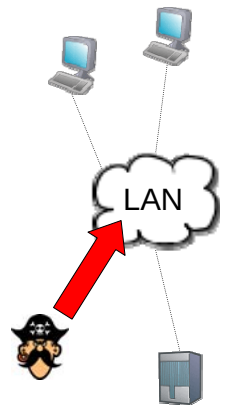
→ Schutz von Management Frames notwendig

IEEE 802.11w Draft 4.0

- 802.11w fügt wichtigen Management-Rahmen einen Message Integrity Code (MIC) hinzu
  - Disassociation, Deauthentication, Action
  - Schutz vor Fälschung
- für Unicast Management-Rahmen wird das bisherige AES-CCMP-Verfahren genutzt
  - paarweise Schlüssel sind notwendig
  - TKIP wird nicht unterstützt
- Multicast/Broadcast Management-Rahmen werden wie mit AES-128-CMAC geschützt
  - AES-128-CMAC authentifiziert Daten mit Hilfe der AES-CBC Verschlüsselungsfunktion
  - Gruppenschlüssel

Schutz von Schicht 2

- Angriffe auf drahtgebundene Netze noch möglich (z.B. Ethernet)
- 802.1X löst nicht alle Probleme
- man hätte gerne noch
  - Geheimhaltung
  - Authentizität
  - Schutz vor Wiederholungsangriffen
  - Schutz vor DoS-Angriffen
- und volle Ethernet-Geschwindigkeit (z.B. 10 Gbit/s) soll erhalten werden

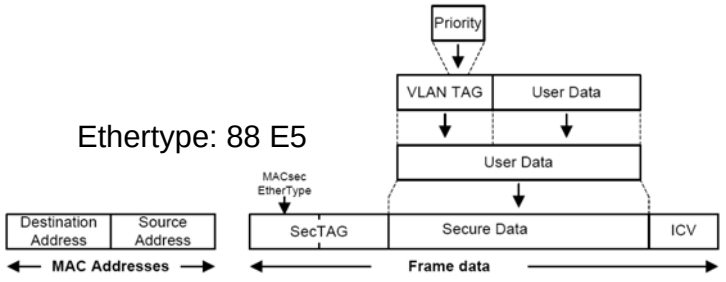


MACsec Übersicht

- IEEE 802.1AE-2006 spezifiziert MACsec
- MACsec bietet (laut Standard)
  - Datenintegrität (Schutz gegen Veränderung)
  - Datenauthentifizierung (Herkunftsschutz)
  - Geheimhaltung (durch Verschlüsselung)
  - Wiederholungsschutz
  - Verzögerungsschutz
- Und damit
  - Schutz gegen Denial-of-Service
  - Aber **keine** Nicht-Abstreitbarkeit
  - Und **kein** Schutz gegen Verkehrsanalyse

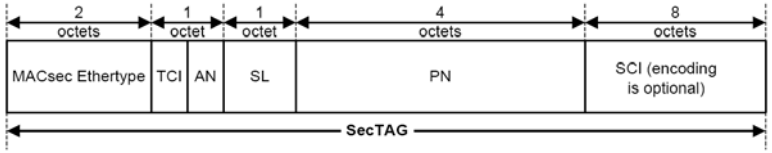
MACsec: Rahmenformat

- MACsec wird mittels verändertem MAC-Rahmen implementiert
  - Vergleichbar mit VLAN-Tags



Quelle: IEEE 801AE-2006

MACsec: SecTAG



- TAG Control Info (TCI)
  - Version, Optionen, …
- Association Number (AN) [2 Bits]
  - 4 verschiedene „SAs“ pro Security Channel
  - erlaubt einfaches Rekeying
  - Rahmen müssen nicht in Reihenfolge sein (beim Umschalten)
- Short Length (SL)
- Packet Number (PN)
- Optionaler Secure Channel Identifier
  - hiermit kann Multicast implementiert werden

MACsec: Zusätzliche Details

- Galois/Counter Mode (GCM) für AES 128
  - Vergleichbar mit CCM-Operationsmodus
- Aber was ist mit Broadcast/Multicast?
  - Mit SCI-Feld realisierbar
  - Ethernet aber zumeist Punkt-zu-Punkt
- Schlüsselautausch?
  - IEEE 802.1af (Erweiterung zu IEEE 802.1X)

Literatur

Bücher

Security in Wireless LANs and MANs, Hardjono und Dondeti, 2005

→ sehr gutes Buch, 802.1X, Radius, PAP, CHAP, EAP-TLS, PEAP, EAP-TTLS, EAP-SIM, EAP-AKA, WEP, 802.11i

Real 802.11 Security, Edney und Arbaugh, 2004

→ sehr ausführliches Buch über 802.11i

802.11 Security, Potter und Fleck, 2002

→ kurzes gutes Buch, leider veraltet

Sichere Netzwerkkommunikation, Bless et al, 2005

→ kurz und prägnant dargestellt

Weitere Literatur

[Wha01]: S. Whalen, *An Introduction to ARP Spoofing*, 2001
http://www.node99.org/projects/arpspoof/arpspoof.pdf

Standards

J. Romkey; *A nonstandard for transmission of IP Datagrams over serial lines: SLIP*; RFC 1055; 1988

W. Simpson; *The Point-to-Point Protocol (PPP)*; RFC 1661; 1994

D. Rand; *The PPP Compression Protocol (CCP)*; RFC 1962; 1996

G. Meyer; *The PPP Encryption Protocol (ECP)*; RFC 1968; 1996

W. Simpson; *PPP Vendor Extensions*; RFC 2153; 1997

G. Zorn, S. Cobb; *Microsoft PPP CHAP Extension*; RFC 2433; 1998

L. Mamakos et al; *A Method for Transmitting PPP Over Ethernet (PPPoE)*; RFC 2516; 1999

B. Aboba, D. Simon; *PPP EAP TLS Authentication Protocol*; RFC 2716; 1999

G. Zorn; *Microsoft PPP CHAP Extension, Version 2*; RFC 2759; 2000

B. Aboba et al; *Extensible Authentication Protocol (EAP)*; RFC 3748; 2004

S. Blake/Wilson et al; *Transport Layer Security (TLS) Extensions*; RFC 4366; 2006

IEEE Standard: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*; 802.11-1999; 1999

IEEE Standard: *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*; *Amendment 6: Medium Access Control (MAC) Security Enhancements*; 802.11i-2004; 2004

IEEE Standard: *Port-Based Network Access Control*; 802.1X-2004 (Revision to 802.1X-2001); 2004