Wireless Security Evolution

WIRELESS FUTURE. UNLEASHED NOW.™

Kevin Hayes

Distinguished Engineer

Atheros Communications

About myself

- Engineer for Atheros Communications since 2000
- Interests in OS and systems design, L2/L3 networking, QoS and security
- Participant/Contributor to IEEE 802.11
  - TGf (Inter Access Point Protocols)
  - TGi (WLAN Security)
  - TGk (Radio system measurement)
  - TGn (High rate WLAN)
  - TGr (Fast, secure handoff)
  - TGs (WLAN mesh)
  - TGw (Security for WLAN Management Frames)

Wireless is Rocking Our World!

Devices

- Traditional WLAN connectivity (laptops, APs)
- CE devices
  - Sony PSP, Microsoft Zune, Satellite+WLAN media players, …
- VOIP phones

Services

- Hotspot connectivity
- Gateways controlled by service providers
- Video distribution – IPTV
- Skype and other voice services
- Other streaming services – iTunes, Rhapsody

See http://www.wi-fi.org for list of WFA certified devices

We’ve been here before

Circa 1994, connection was king, no security awareness

- Connection speed was measurement of connection quality
  - 19.2 Kbps…woo-hoo!
- No e-commerce, No SSL
- Rare for brick-n-mortar enterprise to have Net presence, let alone a firewall

Today, we have reasonable Net security. But the WLAN cometh:

- >60% home wireless networks unsecured
- Wireless usage model presents new opportunities to attackers
- Many more threats than before

Users expect wireless connections to add no new security exposure

We need standards to design security into WLANs

802.11 background

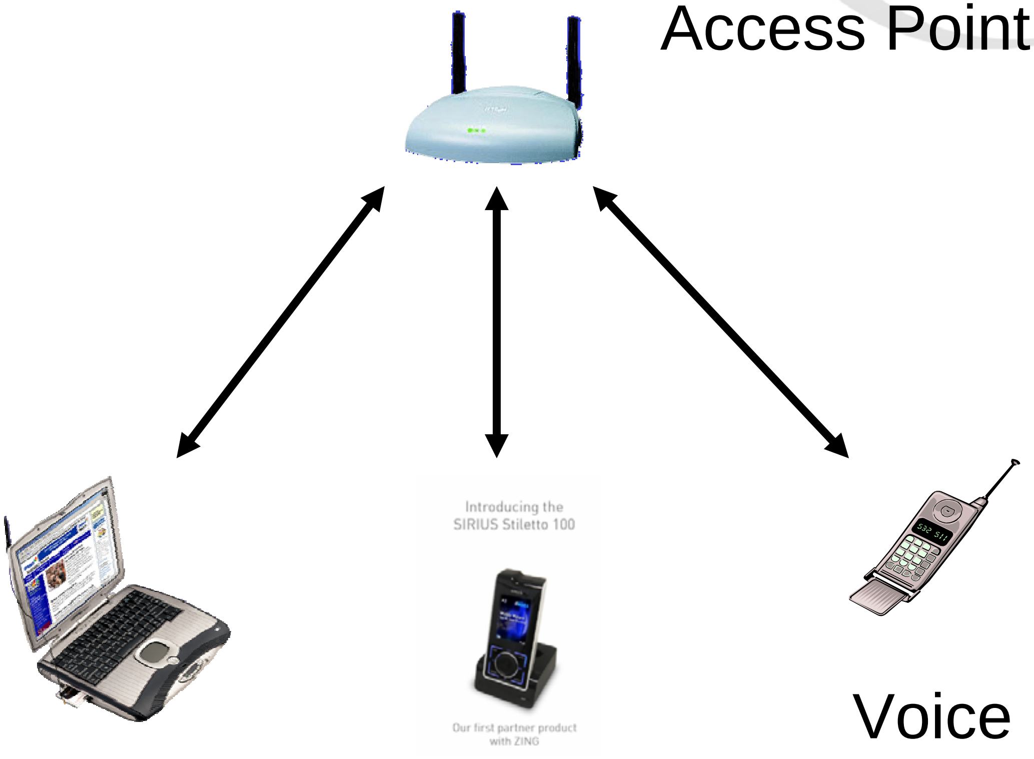
IEEE 802.11 is a subset of IEEE 802 LAN standard

- Uses collision avoidance system
- Provides acknowledged unicast data delivery
- Shared medium allows efficient (unacknowledged) broadcast delivery

Access Point (AP)

- Nexus point of WLAN
- Gateway to other Layer2 services
- Always visible to every node (1st hop)
- Natural point of security enforcement

802.11 Architecture



Access Point

Voice

Data services

Media streaming

Wireless Security Threats

- File theft via unsecure file sharing protocols
- Identity theft
- Viruses
- Rootkits
- Zombie daemons / remote execution
- Spam sourcing and relaying
- Loss of service
  - ISP access
  - Media streaming rights
- System integrity degradation

Tenets of Security

Authentication

- "How do I know you are whom you say you are?"
- Prevents unauthorized *writes* into the network

Key Management

- An agreed-upon, secure way to manage (derive, distribute, utilize) a secret
- Causality/liveness is required!

Confidentiality

- Encryption
- Prevents unauthorized *reads* from the network

Security protocols missing any of these only put lipstick on the pig!

WEP – The classic pig

Poor authentication

- “Shared Key authentication” is less secure than open!
- No per-packet authentication (MIC)
- None of 802.11 frame header protected at all
- No replay checking

Poor key management

- No liveness, no causality
- All key material known to all clients
    - No privacy from other insiders

Poor encryption implementation

- RC4 is a good cipher, but it’s not how good your cipher is, it’s what you do with it…
    - Key stream restarted every packet, IV prepending exposes weakness in RC4

Security – that means IPSEC right?

Nope, in a LAN we can do Port-based Authentication

- Independent of PPP semantics (unlike L2TP)
- No need to obtain L3 resources before authentication
  - No L3 addresses, DNS service, ARP, default router discovery, etc.
- Doesn’t offend IEEE charter sensibilities
  - Works in any IEEE 802 LAN environment (Ethernet, token ring, FDDI, WLAN)
- In WLAN, AP is natural point of enforcement (NAS)

Sweeeeeet!

Umm…what can we use for Port Authentication?

Primordial Ooze: dialup access

In days of yore –

- Users obtained IP access over (gasp!) dialup modem lines
- Modem lines centralized (pooled) at ISP premises
- Access requests flowed through a Network Access Server (NAS) which also served as point of policy enforcement
- NAS usually forwarded requests to a server which actually held the database of user credentials (Authentication Server)
- Usually only session authentication was done, no encryption
- PPP most commonly used as transport, started to have authentication sub-protocols
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)

➡ Extensible Authentication Protocol (EAP)

Assembling the Tools

EAP (RFC 2284) developed by IETF

- Could not simply invoke EAP directly on a LAN
- No IEEE 802 encapsulation until…

IEEE 802.1X – LAN Port Based Authentication (2001)

- Mapped EAP methods onto IEEE 802 LAN-based media
- Glue between IETF (EAP) and IEEE (802 LAN)
- Can transport *any* EAP-based authentication method
- Defined reasonable key management method
- Can transport keys for *any* cipher

RADIUS most popular AAA server

- Most APs use IP as management interface

Some common EAP methods

EAP-MD5

- One-way auth, no PKI, *no confidentiality*

EAP-TLS

- Mutual auth, PKI

EAP-TTLS

- Mutual auth, no PKI on client

EAP-LEAP

- Mutual auth, no PKI

EAP-PEAP/EAP-TLS

- Mutual auth, PKI, cert not exposed

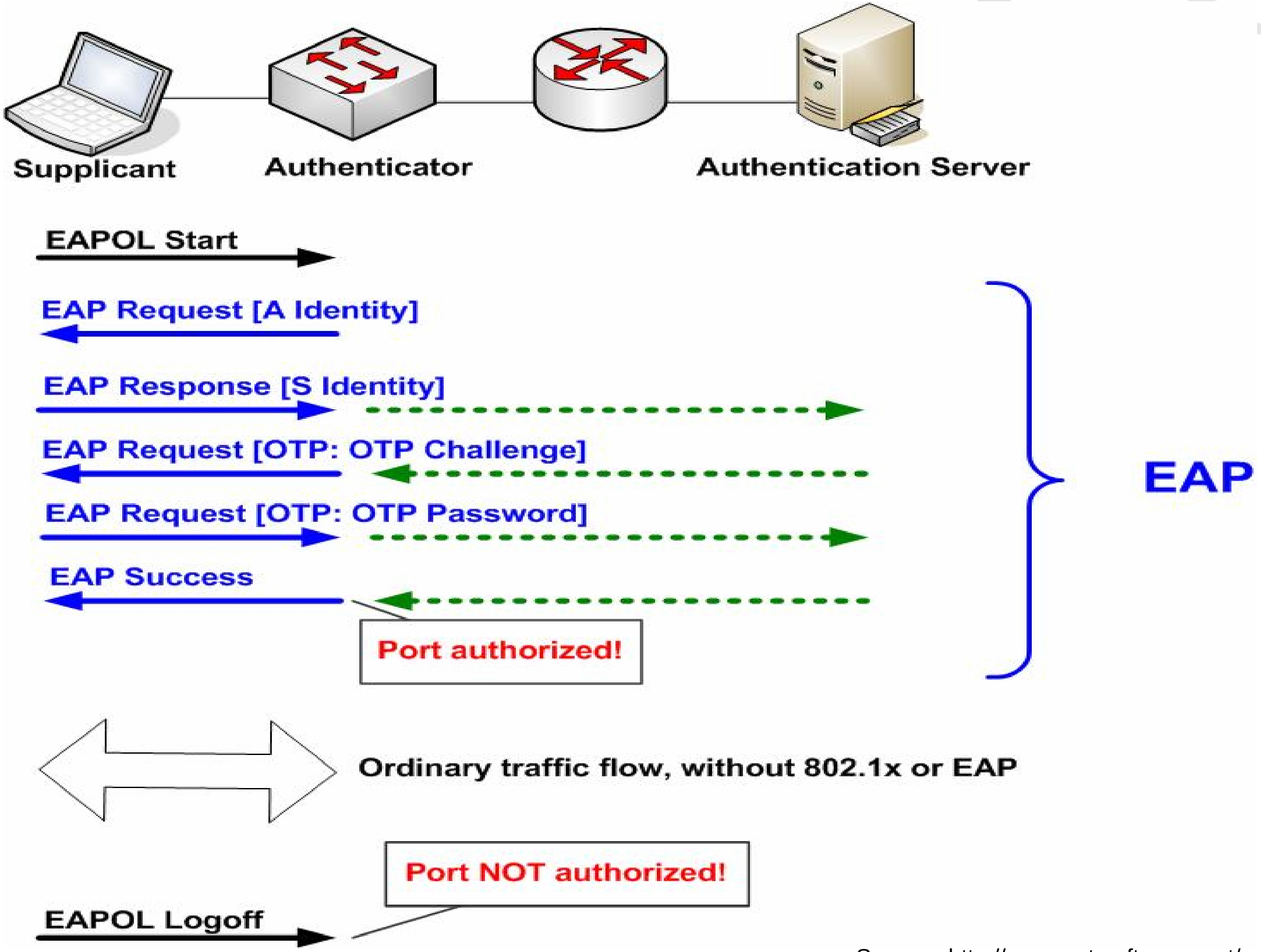
EAP-PEAP/MS-CHAPv2

- Mutual auth, no PKI on client

EAP-PEAP/GTC OTP/tokens

- Mutual auth, no PKI on client, multiple factor

802.1x and EAP



Source: http://www.netcraftsmen.net/welcher/papers/fig200403f.jpg

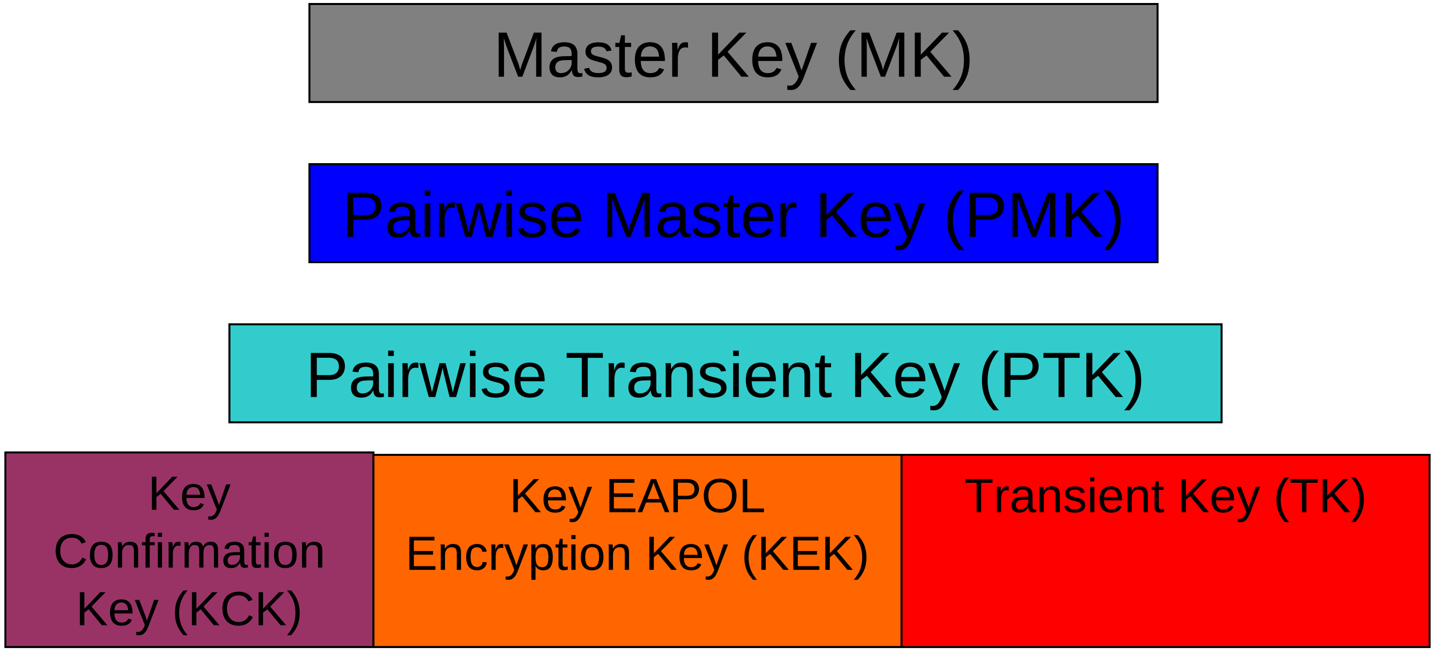
Building the Security Foundation

Security Associations always between exactly two parties

- AP is left out of the party!

We need a hierarchy of keys to provide compartmentalization

- If a device is compromised, security violation is bounded



Master Key (MK)

Pairwise Master Key (PMK)

Pairwise Transient Key (PTK)

Key Confirmation Key (KCK)

Key EAPOL Encryption Key (KEK)

Transient Key (TK)

Toss the AP a bone

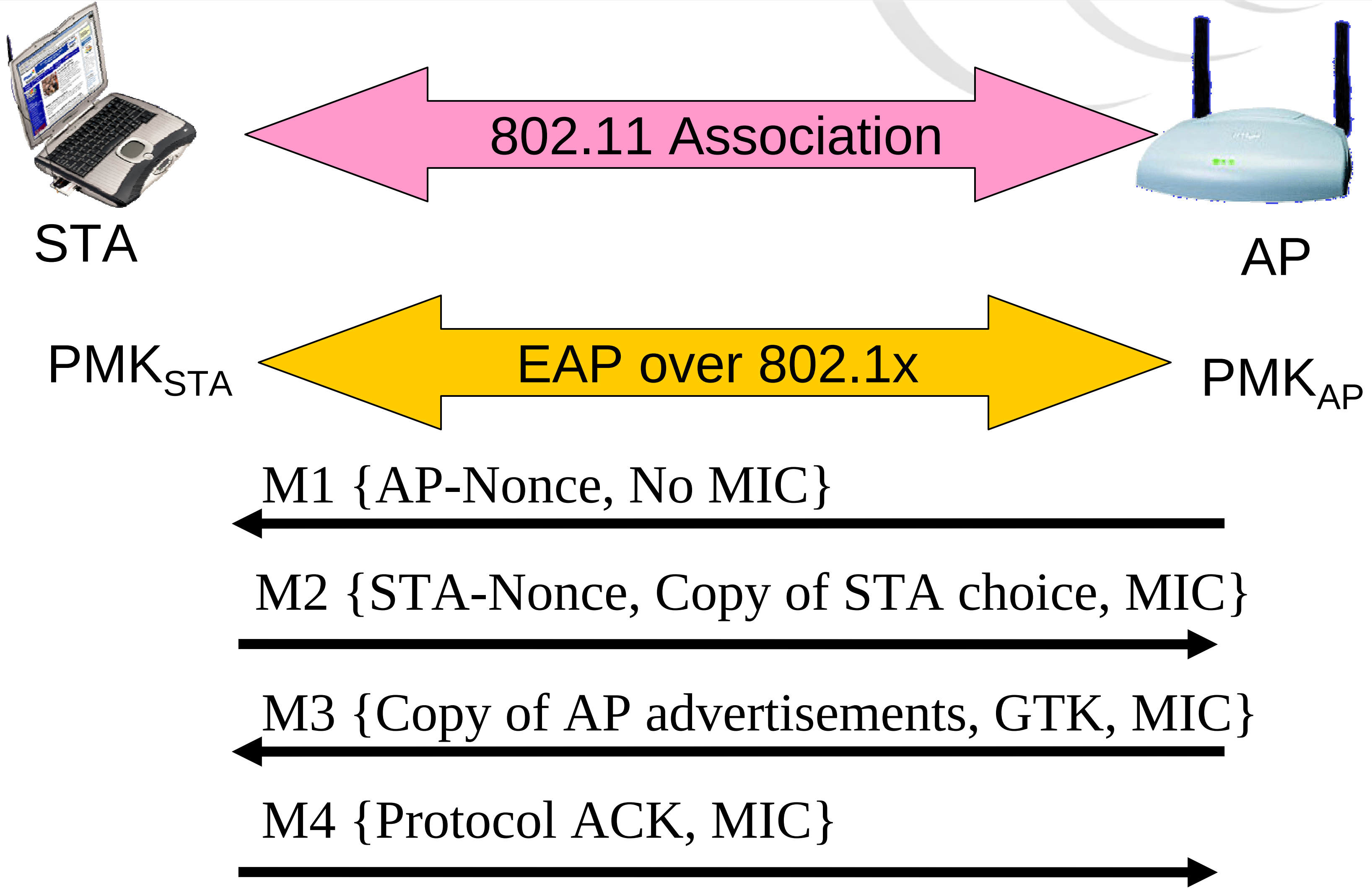
STA and AS derive the PMK

- Still need link-local keys for both unicast and multicast
- How can STA trust the AP?
- How can AP trust the STA?

To Build that trust…

- Both parties assume the other is in possession of the PMK
- AP and STA exchange a session-unique random
- Both entities apply a keyed hash algorithm using the PMK and exchange results
- AP is initiator, responsible for timeout management
- AP may optionally deliver a multicast key

802.11i 4 way handshake



STA

802.11 Association

AP

PMK_{STA}

EAP over 802.1x

PMK_{AP}

M1 {AP-Nonce, No MIC}

M2 {STA-Nonce, Copy of STA choice, MIC}

M3 {Copy of AP advertisements, GTK, MIC}

M4 {Protocol ACK, MIC}

Fixing a hole…

In 2003, vendors required a patch to WEP so they could re-use extant RC4 hardware

TKIP – short term patch

- Key mixing (104 bit per-packet key, 128 bit key for stream)
- 48 bit IV to mitigate key reuse issue
- Replay checking
- “Reasonable” per-packet authentication (MIC)
- Countermeasures (for when attackers figure out limits of “reasonable”)

AES – long term solution

- Required for all newly-certified equipment
- 128 bit per-packet keys, 8 octet MIC, replay checking, more header protection

How will this work at home?

Create PMK from a PSK (passphrase)

PMK can be derived from a one-way transform of passphrase

- Can be very secure!
  - Required mode in FIPS 140-2
  - Key management difficult for humans
- Can be very unsecure!
  - Passphrase can be guessable, subject to dictionary attacks
  - Key management much easier

But most home wireless networks remain in default config

Need security and ease of use!

WFA SimpleConfig protocol

WFA SimpleConfig protocol

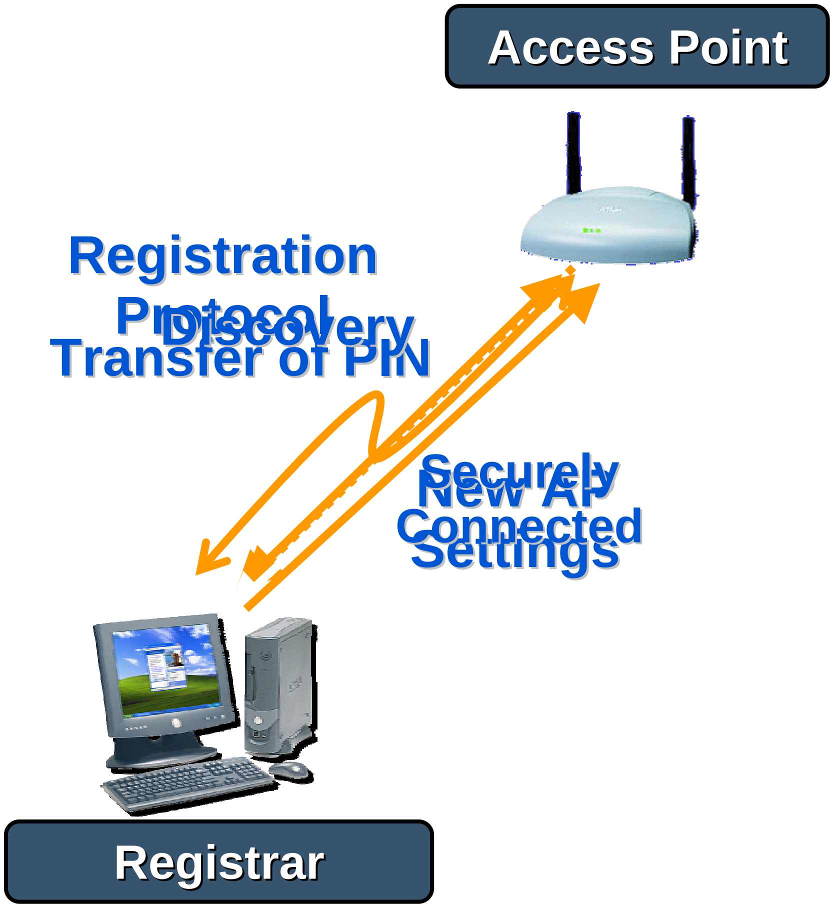
Gives illusion of only two agents

- Registrar
  - Entity responsible for granting and delivery of network credentials
- Enrollee
  - Entity wishing to join the network
- Access Point
  - Sometimes participant, sometimes forwarding agent

Default security level set by equipment vendor

- Authenticated Diffie-Hellman when PIN available
- Unauthenticated Diffie-Hellman when no PIN, but physical access required

WFA Simple Config: Setting up a New Network



Access Point

Registration Protocol

Discovery

Transfer of PIN

Securely Connected

New AP Settings

Registrar

Discovery of New Access Point

Transfer of PIN using OOB mechanism

Registration Protocol runs as EAP method

New AP Settings sent encrypted

EAP – Extensible Authentication Protocol

Coming Security Enhancements

IEEE 802.11 TGk – Radio Measurement

- Network topology discovery
- Scanning enhancements

IEEE 802.11 TGr – Fast BSS Transition

- Overlap security setup with current connection (soft handoff)
- Support for WLAN switch architectures
- Allow expansion of backend key scope (push or pull model)
- Allow pre-reservation of QoS resources (streaming and voice)

Coming Security Enhancements (2)

IEEE 802.11 TGs – Wireless LAN Mesh Networking

- Security across a metro wireless deployment
- Can be adapted to home media streaming environments

IEEE 802.11 TGv – Radio Management

- Diagnostics feedback from authentication processes

IEEE 802.11 TGw – Security for 802.11 Management frames

- Prevent DoS attacks via management frames

Direct Link Session (DLS)

- Security of two peers in a BSS, independent of AP

Virtual AP (multiple BSSID)

- Allows multiplicity of services, security features

Resources

- http://www.drizzle.com/~aboba/IEEE/
- RFC 2284 (EAP)
- RFC 4017 (EAP method requirements for WLANs)
- http://grouper.ieee.org/groups/802/11/
- http://www.raulsiles.com/resources/wifi.html
- http://sourceforge.net/projects/wepcrack
- http://airsnort.shmoo.com/

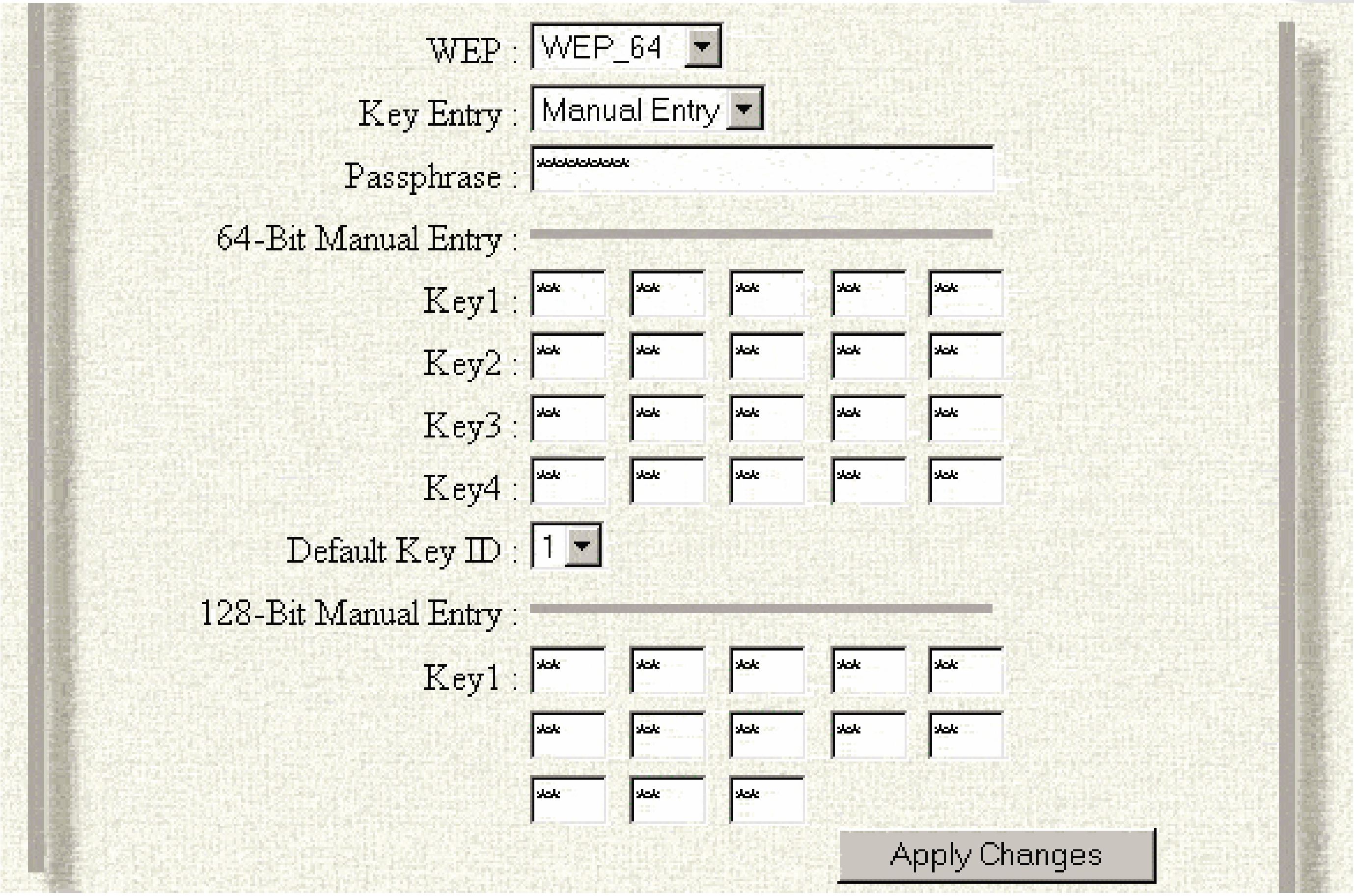
Questions?

Atheros Communications

WIRELESS FUTURE. **UNLEASHED NOW.**™

Backup

WEP example configuration



WEP : WEP_64

Key Entry : Manual Entry

Passphrase : **********

64-Bit Manual Entry :

Key1 : ** ** ** ** **

Key2 : ** ** ** ** **

Key3 : ** ** ** ** **

Key4 : ** ** ** ** **

Default Key ID : 1

128-Bit Manual Entry :

Key1 : ** ** ** ** **
** ** ** ** **
** ** **

Source: http://www.tomsnetworking.com/network/20020719/index.html