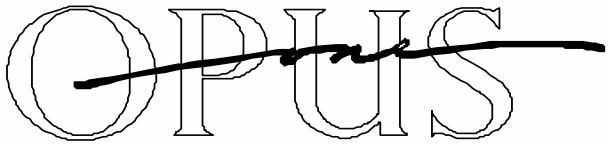
10 Tactics to Build a Secure Wireless Network

Joel M Snyder
Senior Partner
Opus One, Inc.
jms@opus1.com



I'm not here to spread FUD about WLAN Security

It's not as insecure as some folks want you to believe…

- **You can't "break into" a wireless LAN in 15 minutes**
- **It's not trivial to "break into" wireless networks**
- **Adolescents are not decoding your wireless transmissions at 30 MPH**

On the other hand…

- **Compared to other networking we do, wireless has the least inherent security**
- **Denial-of-Service is a real danger from intentional and unintentional sources**
- **You will have to work harder with wireless networks to gain the same level of security you get in other environments**

Six pages of security in 802.11 don't help

The SSID is not a security feature and hiding it won't do you any good (but it will bother everyone who tries to use your LAN)

Sniffer Wireless - Local, 802.11 Wireless LAN DS Channel 1 - Signal Level 79 % - [Snif2: Decode, 195/336 802.11 LANs Frames]

File Monitor Capture Display Tools Database Window Help

Default

No.	Status	Source Address	Dest Address	Summary	Len (B	Rel. Time	Delta Time
195	[1]	Airont31669C	Airont500292	802.11: 1.0 Mbps, Signal=100%, Probe response	52	0:00:08.434	0.000.649

```
DLC:                          .... ..0. = Independent Basic Service Set is off
DLC:                          .... 00..   = No point coordinator at Access Point
DLC:                          ...1 .... = Privacy
DLC:                          ..0. .... = Short Preamble option is not allowed
DLC:                          .0.. .... = Packet Binary Convolutional Coding Modulation mode option is not allowed
DLC:                          0... .... = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC:                          0000 0000 = Reserved
DLC:
DLC: Element ID                     = 0 (Service Set Identifier)
DLC: ...Length                      = 5 octet(s)
DLC: ...Service Set Identity        = "LINC5"
DLC:
DLC: Element ID                     = 1 (Supported Rates)
DLC: ...Length                      = 4 octet(s)
DLC: ...Supported Rates information field = 82
DLC:                             1... .... = Basic Service Set Basic Rate
```

```
00000000: 50 00 3a 01 00 40 96 50 02 92 00 40 96 31 66 9c P.:..@▌P.´.@▌1f▌
00000010: 00 40 96 31 66 9c a0 17 c7 46 39 22 cc 00 00 00 .@▌1f▌ .ÇF9"Ì...
00000020: 64 00 11 00 00 05 4c 49 4e 43 35 01 04 82 84 8b d.....LINC5..▌▌▌
00000030: 96 03 01 01                                     ▌...
```

Expert | Decode | Matrix | Host Table | Protocol Dist. | Statistics

For Help, press F1 201

Denial of service attacks are unstoppable

No standardized security proposal for 802.11 does anything about the poor state of management

Source	Destination	BSSID	Data R...	Cha...	Signal	Flags	Size	Absolute Time	Protocol
00:40:96:5B:37:AF	Broadcast	00:40:96:5B:37:AF	11.0	1	70%	*	30	03:57:59.011112	802.11 Deauth
00:40:96:5B:37:AF	Broadcast	00:40:96:5B:37:AF	11.0	1	77%	*	30	03:57:59.011459	802.11 Deauth
00:07:85:92:DB:A9	Broadcast	Broadcast	1.0	1	90%	*	44	03:57:59.024358	802.11 Probe Req
00:40:96:5B:37:AF	00:07:85:92:DB:A9	00:40:96:5B:37:AF	1.0	1	98%	*	91	03:57:59.025430	802.11 Probe Rsp
	00:40:96:53:37:AF		1.0	1	100%	#	14	03:57:59.025739	802.11 Ack
00:07:85:92:DB:A9	Broadcast	Broadcast	1.0	1	100%	*	44	03:57:59.062430	802.11 Probe Req
00:40:96:5B:37:AF	00:07:85:92:DB:A9	00:40:96:5B:37:AF	1.0	1	98%	*	91	03:57:59.063523	802.11 Probe Rsp
	00:40:96:53:37:AF		1.0	1	100%	#	14	03:57:59.063758	802.11 Ack
00:40:96:5B:37:AF	00:07:85:92:DB:A9	00:40:96:5B:37:AF	1.0	1	88%	*	91	03:57:59.065194	802.11 Probe Rsp
00:07:85:92:DB:A9	Broadcast	Broadcast	1.0	1	81%	*	44	03:57:59.100279	802.11 Probe Req
00:40:96:5B:37:AF	00:07:85:92:DB:A9	00:40:96:5B:37:AF	1.0	1	96%	*	91	03:57:59.101339	802.11 Probe Rsp
00:40:96:5B:37:AF	Broadcast	00:40:96:5B:37:AF	11.0	1	79%	*	30	03:57:59.113531	802.11 Deauth
00:40:96:5B:37:AF	Broadcast	00:40:96:5B:37:AF	11.0	1	77%	*	30	03:57:59.113932	802.11 Deauth
00:07:85:92:DB:A9	Broadcast	Broadcast	1.0	1	72%	*	44	03:57:59.138173	802.11 Probe Req
00:40:96:5B:37:AF	00:07:85:92:DB:A9	00:40:96:5B:37:AF	1.0	1	79%	*	91	03:57:59.139230	802.11 Probe Rsp

... and the microwave oven in your break room really does act as an effective tool for shutting down local access

Here's the easy answer: 802.11i: Robust Security for Wireless Networks

- **IEEE developed 802.11 supplement "Specification for Robust Security" in Task Group I (802.11i)**
- **Improved security with deployed hardware**
- **Complete "robust" security: whole new model**
- **Approved: July 29th, 2004**
- **First products certified: September, 2004**

802.11i represents IEEE "fixing" of 802.11 security

- **Temporal Key Integrity Protocol (TKIP)**
  - **Enhances WEP to provide a per-packet rekeying mechanism**
  - **Adds a Message Integrity Check (MIC) field to packet to stop packet tampering—also adds break-in evasion features in the MIC**
  - **Needs 802.1X to provide base key change mechanism**
- **Advanced Encryption Standard (AES)**
  - **Replaces RC4 in WEP**

Wi-Fi Protected Access(WPA) calls for a subset of 802.11i

If 802.11i is the way to go, why is this talk so long?

- **802.11i is the last word from the IEEE on securing wireless networks**
- **802.11i includes strong user authentication to ensure**
  - **You are who you say you are**
  - **You are talking to the access point you want to**
- **802.11i includes a "good" encryption algorithm**
  - **People have not poked holes in AES yet**
- **802.11i even includes per-message authentication**

So with all this good stuff, why isn't the answer "put in 802.11i and be done with it?"

I have one word for you: "legacy"

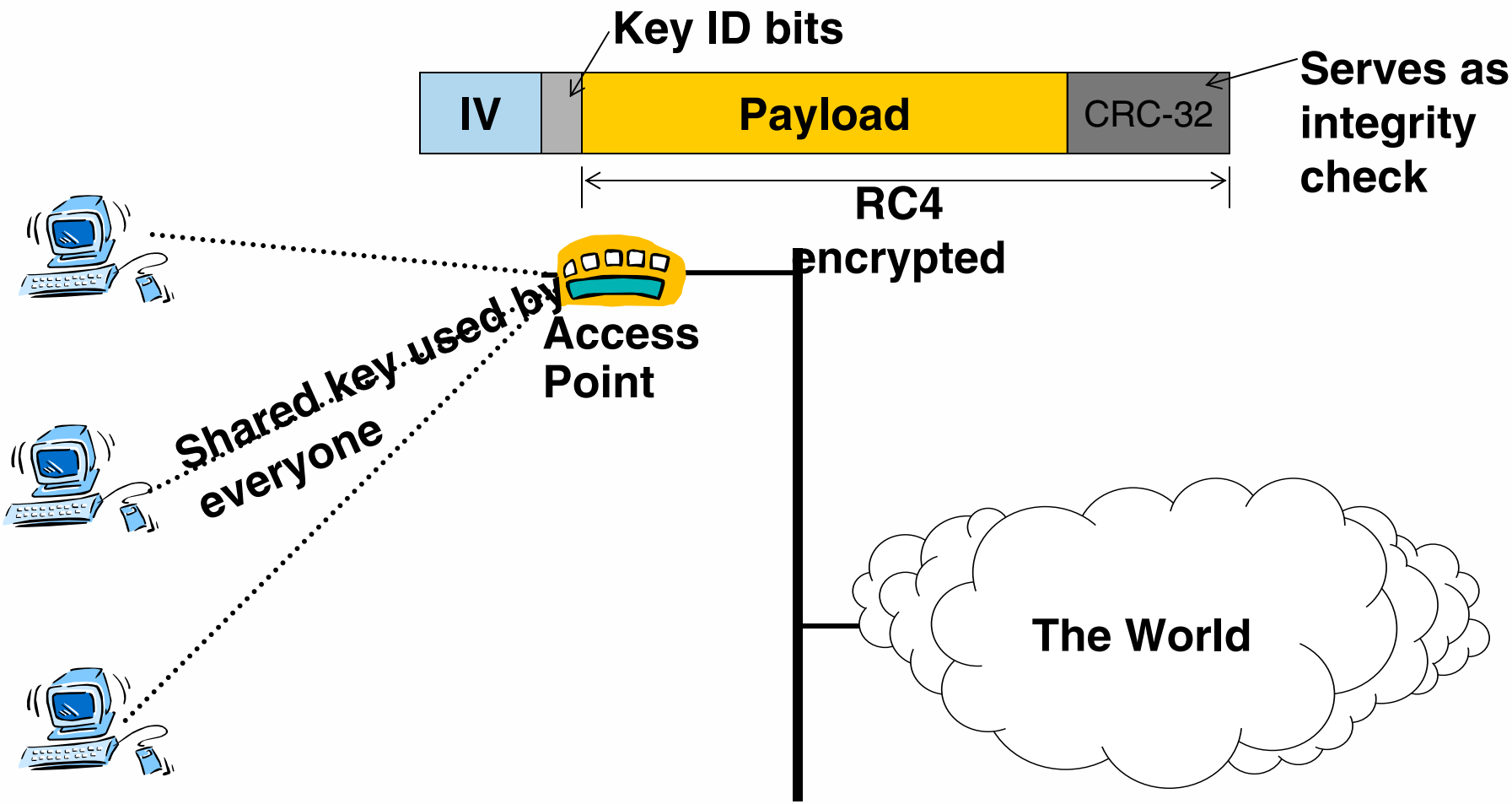
- **Legacy equipment may not be capable of AES encryption**
- **Legacy equipment may not be capable of 802.1X authentication**
  - **Actually, new equipment may not do that either**
- **In fact, Legacy equipment may not be able to do anything smarter than WEP**

For the purposes of this discussion,
Guests == Legacy

Wired equivalent privacy is the built-in option

- **Designed to provide security equivalent to a wired network**
- **Uses shared WEP key of 40 bits**
  - **Nonstandard, but common, extension uses 104 bits**
- **Uses an initialization vector (IV) of 24 bits—client changes this every packet and is included in the packet in the clear**
- **Combined IV+WEP key gives a key size of 64 or 128 bits**
- **Packet includes a integrity check value (ICV)—basically a CRC check**
- **Provides encryption but no user or per-packet authentication**

How does WEP work?



Known WEP vulnerabilities

- **40-bit WEP key**
- **Weak IVs**
- **IV Replay**
- **Known packet attack**
- **Known packet start attack**
- **Bit Flipping attack**
- **Management**

Wireless vendors have abandoned WEP

Wireless vendors have jumped on the WPA (PSK or 802.1X) bandwagon and are not interested in anything 'legacy' anymore

See "Cracking the Wireless Security Code" (http://www.nwfusion.com/reviews/2004/1004wirelessmain.html)

Testing WEP security

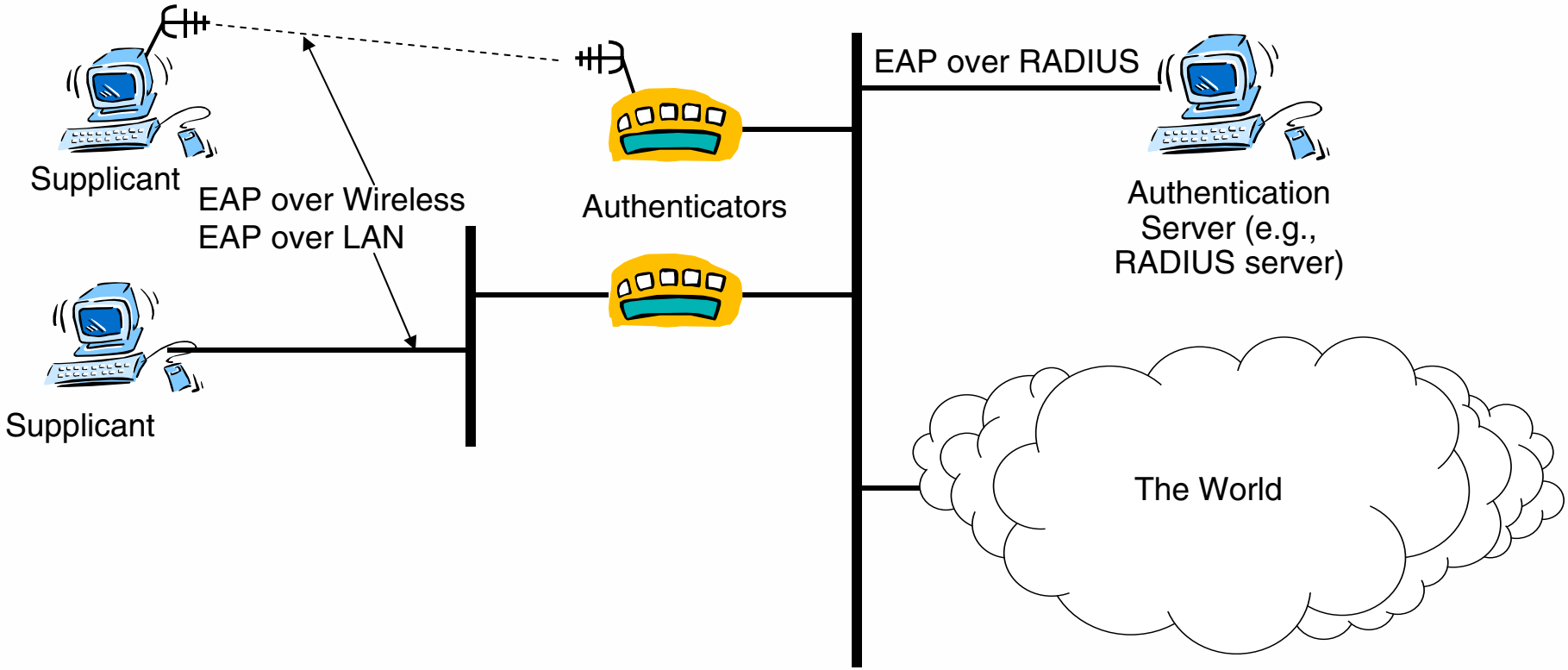
Support for a wide variety of WEP flavors is common in access points, wireless switches and network interface cards, but many of the products we tested are very vulnerable to the 3-year-old key recovery technique available in the AirSnort tool.

Type	Vendor	AirSnort results	WEP key support	Supports weak WEP passphrase feature*
Wireless adapters	3Com	Pass	40-, 104-, 128-bit keys	Yes
	Actiontec	Fail	40-, 104-, 232-bit keys	No
	Apple	Pass	40-, 104-bit keys	Yes
	Belkin	Pass	40-, 104-bit keys	No
	Buffalo	Pass	40-, 104-bit keys	No
	Cisco	Pass	40-, 104-bit keys	No
	Linksys	Fail	40-, 104-, 128-bit keys	No
	SMC	Fail	40-, 104-, 128-bit keys	No
Wireless access points	3Com	Pass	40-, 104-, 128-bit keys	Yes
	Actiontec	Fail	40-, 104-, 232-bit keys	No
	Belkin	Pass	40-, 104-bit keys	Yes
	Buffalo	Pass	40-, 104-bit keys	No
	Cisco	Fail	40-, 104-bit keys	No
	Compex	Fail	40-, 104-bit keys	No
	HP	Fail	40-, 104-, 128-bit keys	No
	Linksys	Pass	40-, 104-bit keys	Yes
	Netgear	Fail	40-, 104-, 128-bit keys	Yes
	Netopia	Fail	40-, 104-, 232-bit keys	Yes
	Proxim	Fail	40-, 104-, 128-bit keys	No
	SMC	Pass	40-, 104-, 128-bit keys	No
Wireless switches	Airespace	Pass**	40-, 104-, 128-bit keys	No
	Aruba	Pass**	40-, 104-bit keys	No
	Trapeze	Pass**	40-, 104-bit keys	No

The worst WEP vulnerability: Management!

- **WEP keys are generally static**
- **WEP keys are shared among lots of users**
- **WEP keys are passed around and are hard to change**
- **This is roughly the same as giving everyone in the company the same password and then refusing to let anyone change it!**

802.1X gives link layer authentication



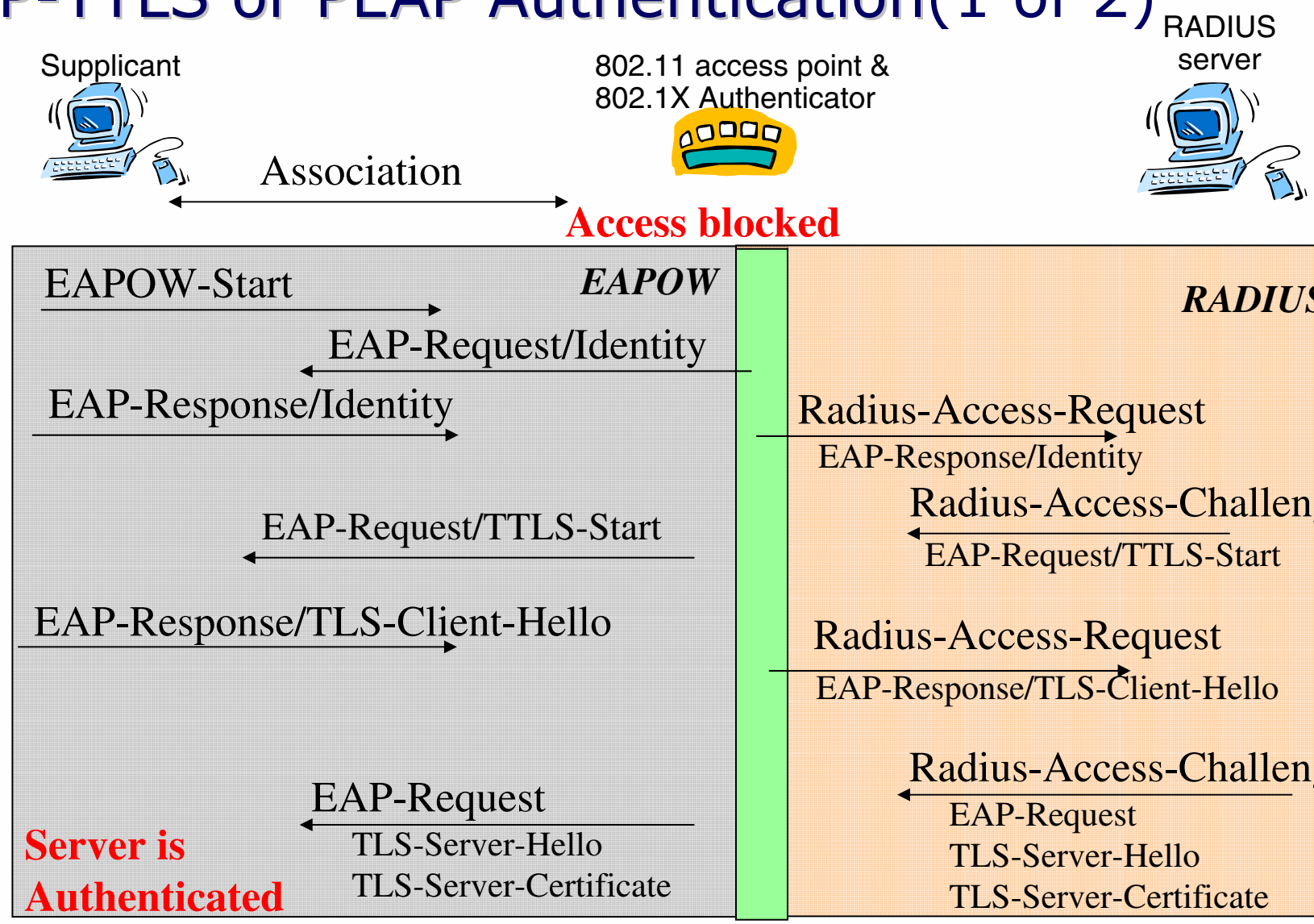
802.1X has special support for wireless communications

- **When properly used with a TLS-based authentication mechanism, you get per-user/per-session WEP keys**
  - **TLS (certificates for user and authentication server)**
  - **TTLS or PEAP (certificates for [illegible] server; legacy authentic[illegible]**

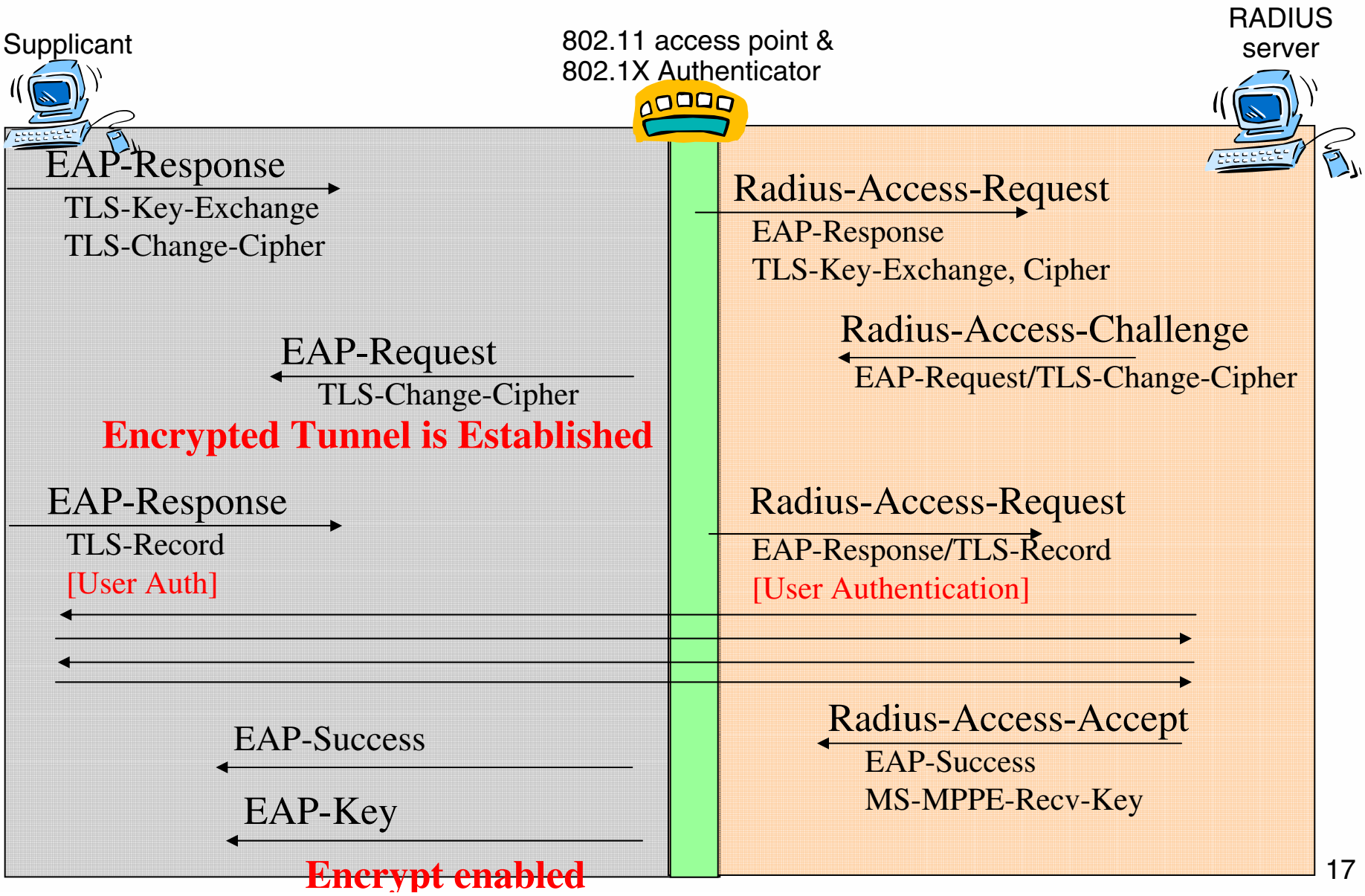
Our good friends in the IETF are doing a great deal of harm here…

Source: B. Aboba

EAP-TTLS or PEAP Authentication(1 of 2)



EAP-TTLS or PEAP (2 of 2)

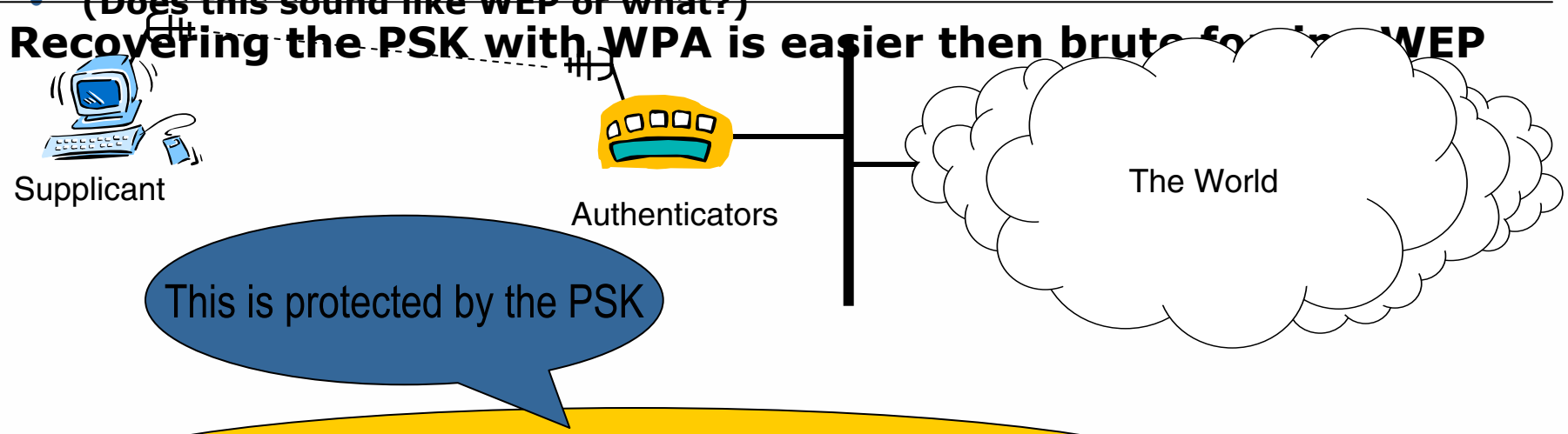


Wi-Fi's WPA

- **Wireless Ethernet Compatibility Alliance (WECA), AKA Wi-Fi Alliance initially provided 802.11 interoperability certification**
  - **Board Members**
    - **Agere, Cisco, Dell, Intermec, Intel, Intersil, Microsoft, Nokia, Philips, Sony, Symbol, TI**
- **Have provided an "interim standard" for 802.11 security: Wi-Fi Protected Acess (WPA)**
  - **Immediate interoperability without waiting for IEEE 802.11i**
  - **WPA 1.2 is portions of 802.11i, Draft 3.0**
    - **Uses TKIP, but not AES-CCMP (or WRAP)**

WPA comes in two flavors: Bad Security and Good Security

- **Bad Security (aka "WPA Personal") doesn't use 802.1X authentication**
- **The per-session encryption key is derived from the non-authentication dialog**
- **The non-authentication dialog is based on the "PSK" (pre-shared key) that everyone knows and you never change**
  - **(Does this sound like WEP or what?)**
- **Recovering the PSK with WPA is easier then brute force in WEP**

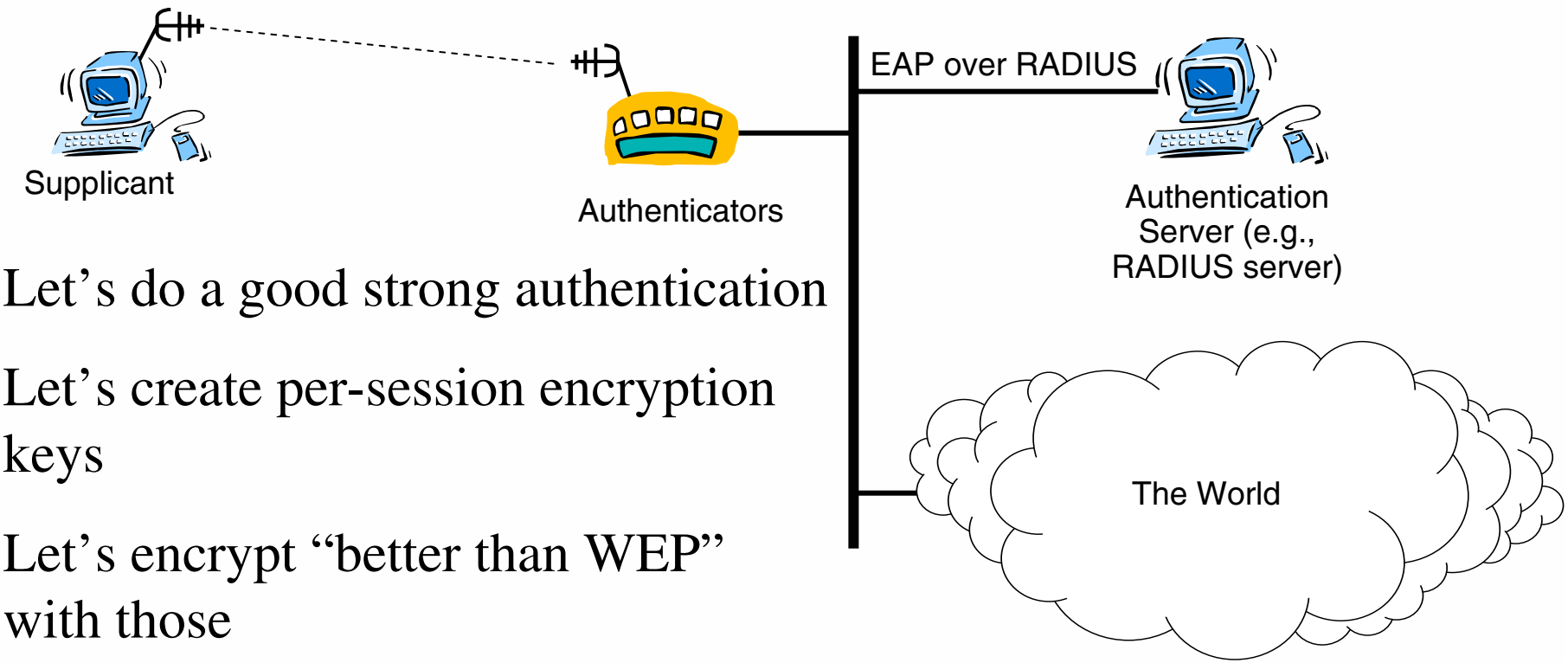


1. Let's agree on an encryption key for this session.
2. Let's use better encryption than WEP to ensure privacy

WPA *Good Security* is not bad

WPA Enterprise is

- **802.1X Authentication**
- **TKIP Encryption**



1. Let's do a good strong authentication
2. Let's create per-session encryption keys
3. Let's encrypt "better than WEP" with those

Let's lay it all out for you

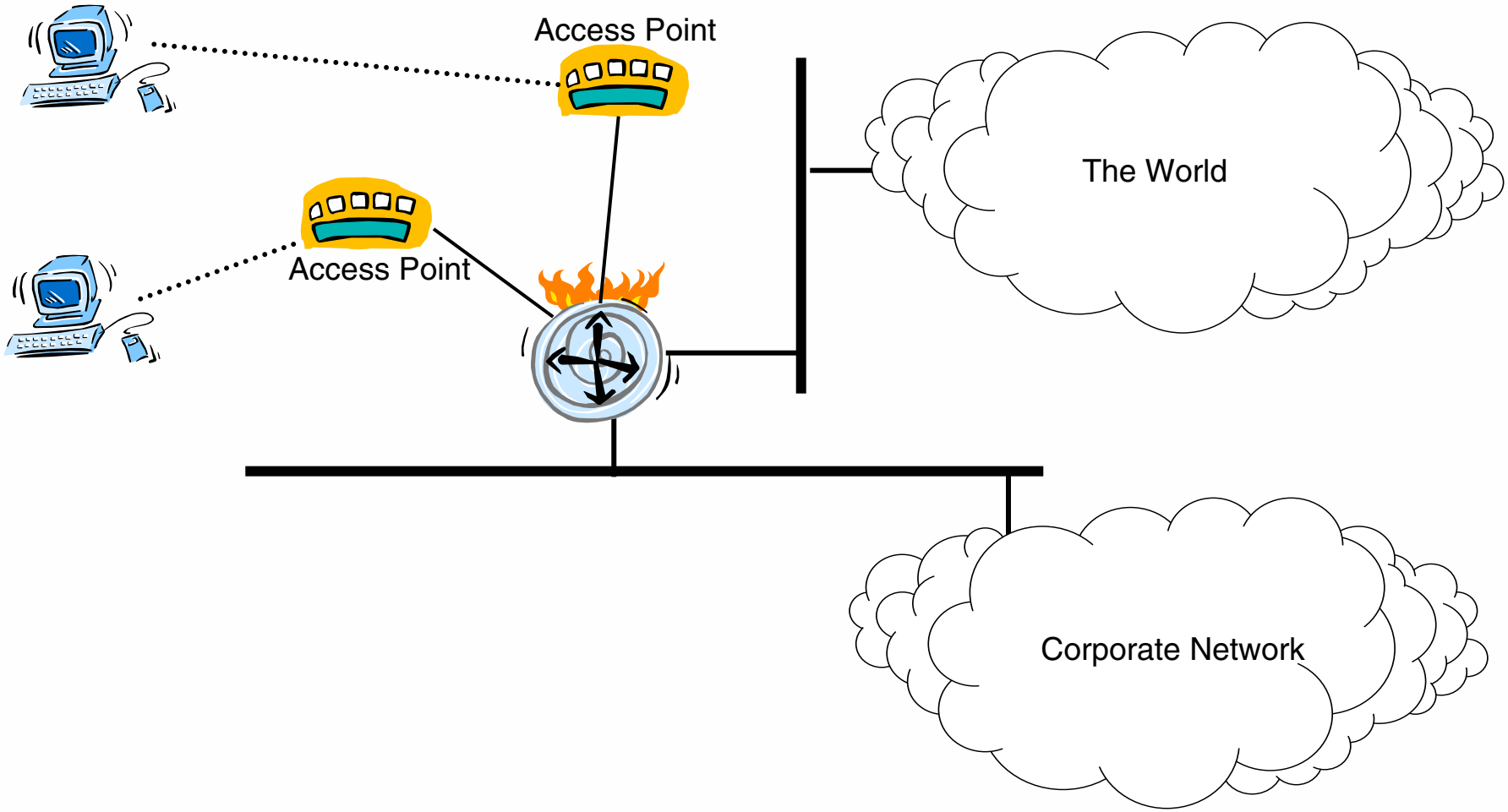
Strategy	Encryption	Authentication	Verdict
WEP40 / 104	WEP, 40-bit keys or 104-bit keys	None	Better than a sharp stick in the eye
802.1X	WEP/104 with per-session keys	Strong 802.1X authentication	Very good
WPA Personal	TKIP with per-session keys	"Pre-shared Key"	Ptui!
WPA Enterprise	TKIP with per-session keys	Strong 802.1X authentication	That's more like it!
802.11i	AES with per-session keys	Strong 802.1X authentication (*)	As good as it's going to get

But what do we do about legacy users?

Answer: Mix and Match!

- **We want to authenticate them**
- **We want to encrypt their traffic**

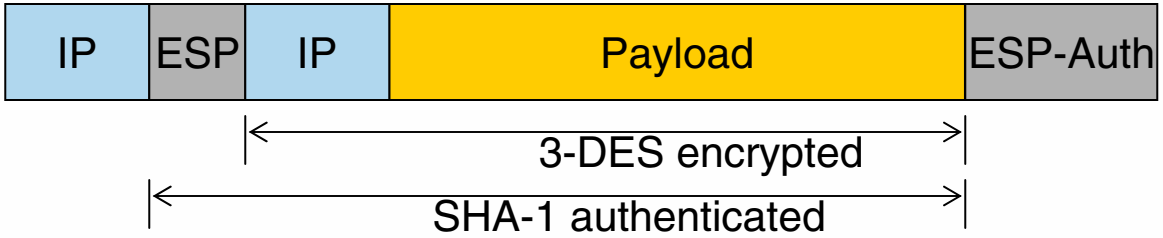
Captive Portal is a strategy for controlling access

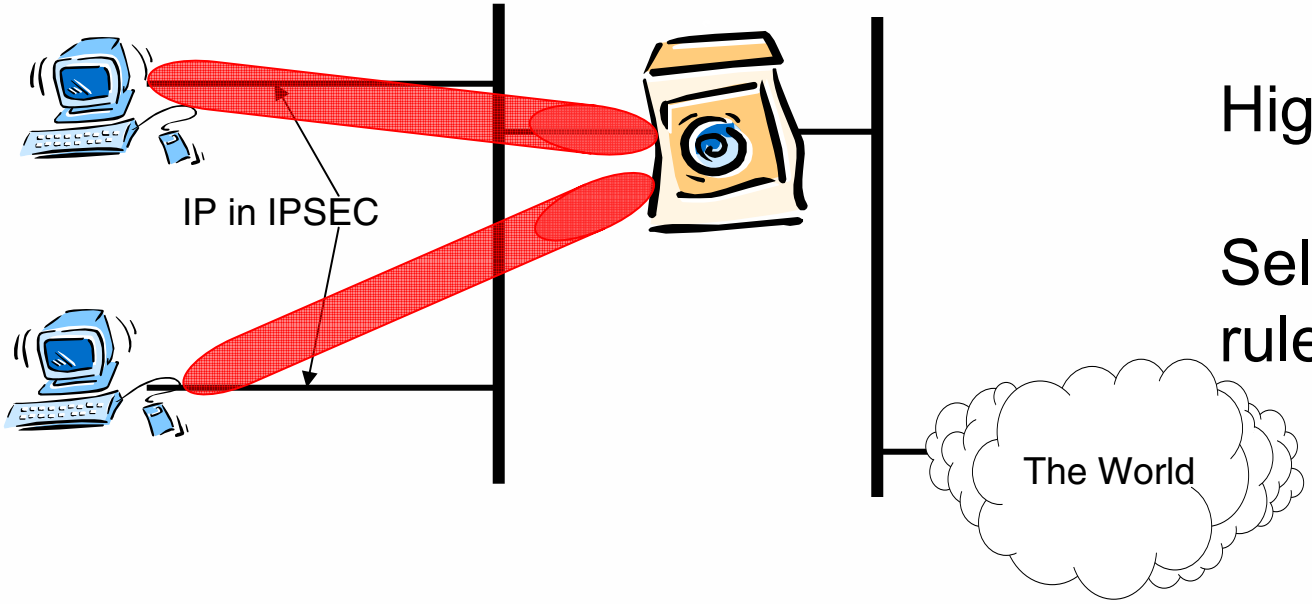


Captive Portal does not offer good security

- **A wide variety of vendors are bringing products to market based on solving the problem without doing the hard work**
- **You can use this technique and maintain security**
  - **If you're willing to play with the access points**
  - **Say "hello" to Airespace (now Cisco), Aruba, etc.**
- **Sometimes you'll take this tack if you define "security" differently**
  - **Plausible deniability in an academic setting**
- **Sometimes captive portal is a useful adjunct for keeping the casual user off your wireless LAN**

IPsec gives serious security





Positive bi-directional authentication of user and gateway

Per-packet encryption and authentication

High re-key rate

Selector-based firewall rules

So many choices, so little time...

Solution	Pros	Cons
WEP	**Very compatible; easy to set up**	**Questionable security; changing keys difficult; other security flaws**
802.1X	**User authentication; per-session WEP key; useful in wired and wireless**	**Need client (supplicant); need new RADIUS server**
802.11i / WPA	**802.1X + better encryption + per-packet authentication + DoS evasion**	**Need new hardware**
Captive Portal	**Most compatible; ultra easy to use**	**Very weak security; easy to hijack, eavesdrop**
IPsec	**Strongest security model; use same model for wireless as Internet remote**	**Need client software; deployment and updating hard** **Lousy encryption; lousy**

Strategies to Secure Wireless LANs

Joel M Snyder
Senior Partner
Opus One, Inc.
jms@opus1.com