Wireless LAN Security:
Where Do We Go From Here?

Michael Disabato
Senior Analyst
Burton Group
mdisabato@burtongroup.com
www.burtongroup.com

December 5, 2002

Burton Group DRIVING NETWORK EVOLUTION™

How We Got Here

WEP has been shown to have some serious weaknesses

- A single key for all access points and client radios
- Keys can be recovered with easily available utilities
- Recovered keys expose the network to attacks
- Lack of automated key management contributes to infinitely key lifespan in large networks
- Most of all….

Equipment is shipped with encryption disabled!!!!

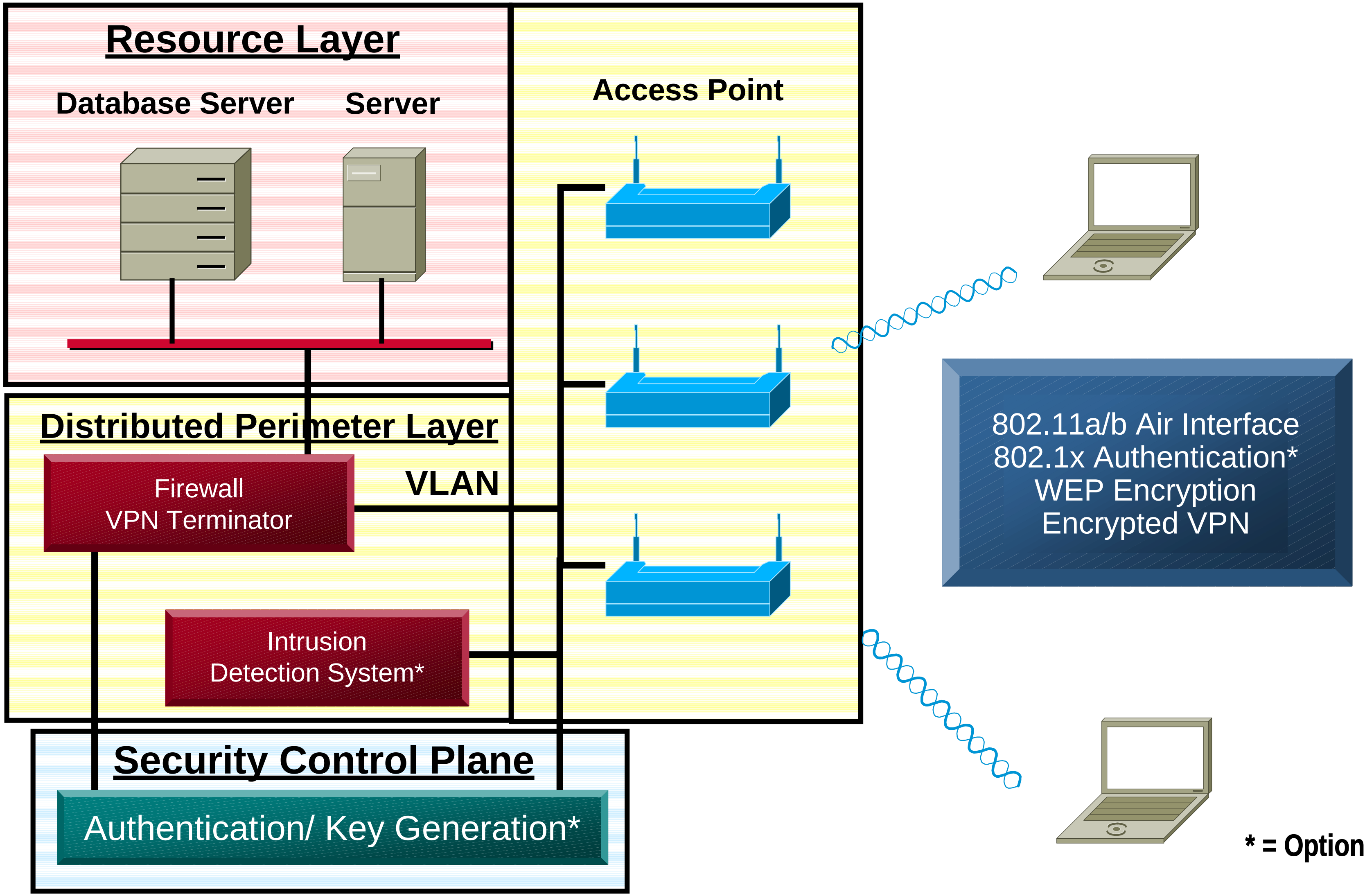
The Quick Fix

Dynamic Key Change

- WLAN vendors implemented the key management that should have been there in the first place
- None of the implementations were compatible
- All the implementations required an authentication server
- Small sites, home networks, enterprises without authentication servers were left out of the solution

This was not a good idea!

Today's Secured Wireless LAN

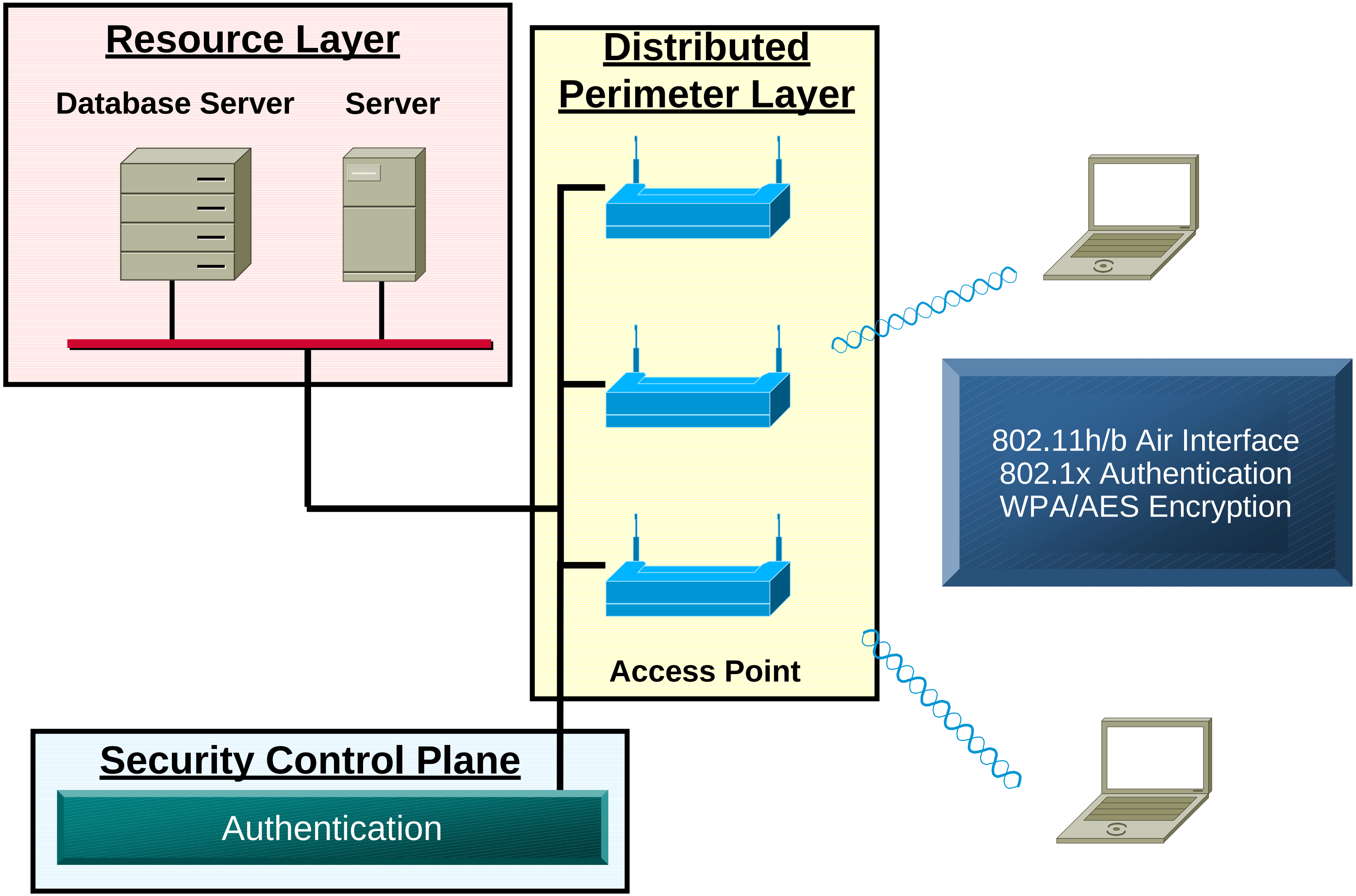


* = Optional

The Promise of WPA

- Software upgrade
- Inexpensive
- Cross-vendor compatible
- Works with authentication server or stand-alone
- Suitable for enterprise, small sites, home networks
- Available now

Tomorrow's Secured Wireless LAN?



Resource Layer

Database Server

Server

Distributed Perimeter Layer

Access Point

802.11h/b Air Interface
802.1x Authentication
WPA/AES Encryption

Security Control Plane

Authentication

Moving Forward

What vendors and Wi-Fi Alliance need to do

- Expedite the delivery of WPA (est. February ‘03)
- Ship all new equipment disabled (until properly configured) in the enterprise space
- Ship all new equipment enabled (proper configuration encouraged) in the residential space

Why should I upgrade to AES?

- There will be a cost in new hardware (mixed, vendor-specific)
- My risk analysis does not warrant the extra protection
- WPA has not been broken; let’s break it
- Not sure if it will have PSK mode
- No compelling business reason to do so

Concluding remarks

What should this group of persons from the IEEE TGi, WiFi Alliance, Federal Government, and security experts need to do about the future of the WiFi industry?

- Perform security research on how to break WPA and develop effective attacks that will motivate to RSN
- Develop advice for proper use of WPA (like 800-48)
- Evangelize to drive organizations off WEP and that long-term solution, RSN, is coming
- Develop forum of IEEE, IETF, 3GPP to harmonize efforts around WiFi
- Review RSN to make sure it is what it should be and develop contributions/changes to draft 3.0