



# Welcome!

*“WPA: The Latest 802.11 Security”*

by Jim Weikert, Product Manager, ProSoft Technology

**ISA 2004**

# Using a Good Tool Improperly





# Concepts to Understand

- Authentication
  - Verifying only authorized users are allowed to communicate
- Encryption
  - Scrambling the data so that it cannot be deciphered by outsiders
- Integrity Checking
  - Preventing unwanted data



# The Good Tool Used Properly

- 802.11 WEP encryption is based on a very strong and time-proven algorithm
- Algorithm is used throughout the world in some of the most secure applications
  - SSL (Secure Socket Layer) Protocol is used for communications to and from secure websites
  - Oracle SQL



# The Good Tool Used Improperly

- WEP is an example of using a good tool improperly
  - Poor authentication (rogue access point)
  - Poor key generation (cracked encryption key)
  - Poor duplicate checking (replay attacks)



# 802.11 Industry Improvements

- IEEE 802.11i
  - New IEEE standard for 802.11 security
- WPA (Wi-Fi Protected Access)
  - The 802.11 industry's acronym for the improved security

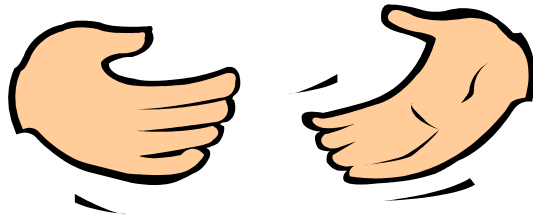


# The Good Tool Used Properly

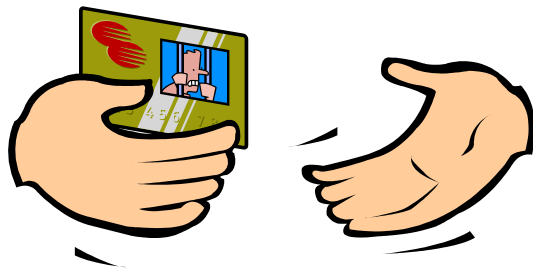
- Proper Authentication
- Proper Encryption

# WPA: Proper Authentication

WEP

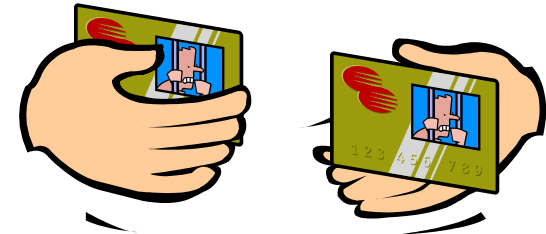


Open



Shared

WPA



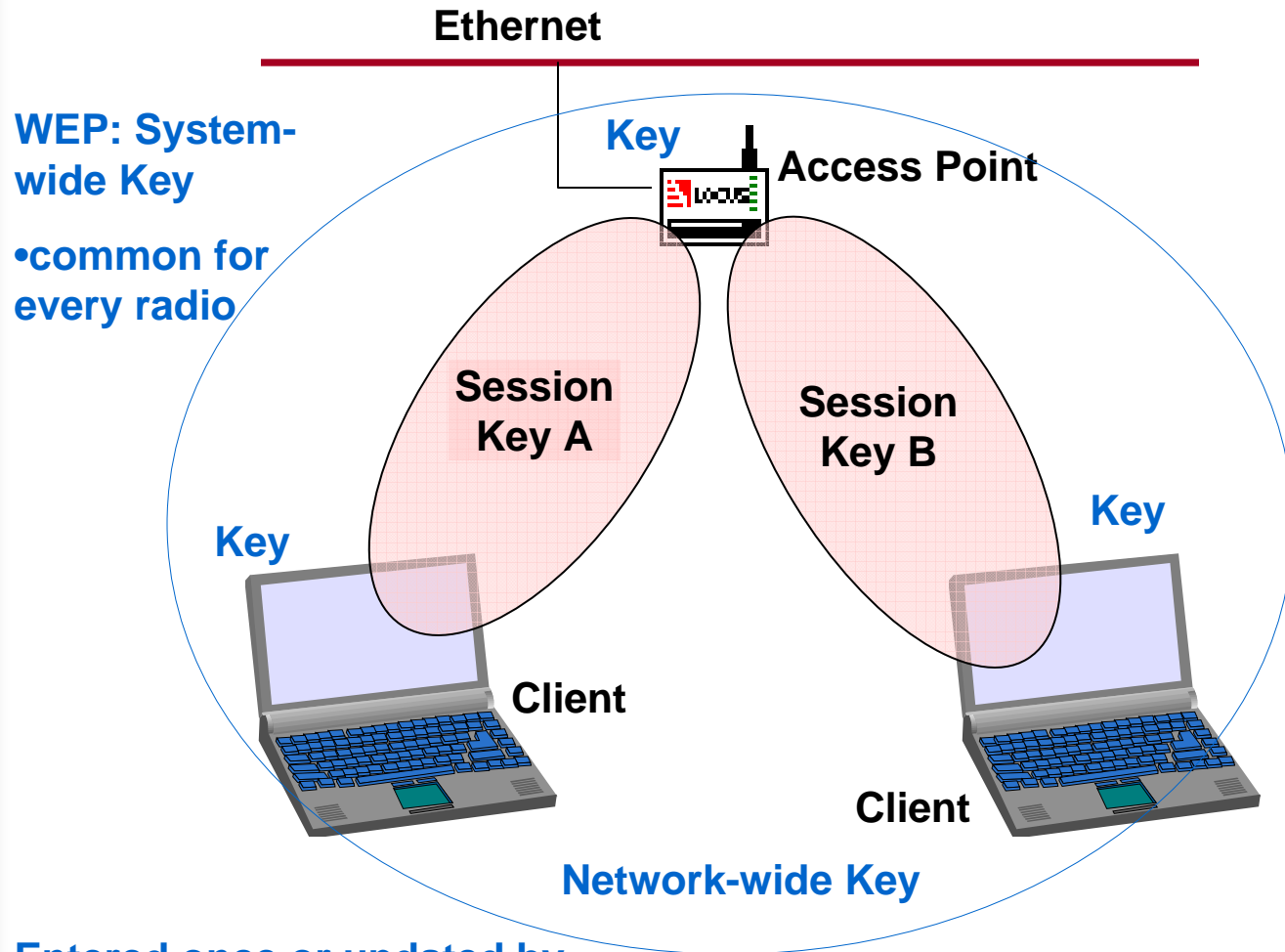
Dual Authentication  
Two-way Handshake



# WPA: Proper Authentication

- WEP shared
  - Only client authenticated itself to AP
  - “Rogue” AP could cause client to authenticate to it falsely and gain access to client’s information
- Dual authentication
  - Client and AP authenticate each other, verifying the link is appropriate

# Key Generation



**WEP: System-wide Key**

- common for every radio

**WPA Session Key:**

- different for every pair
- different for every station
- generated for each session
- derived from a “seed” called the passphrase

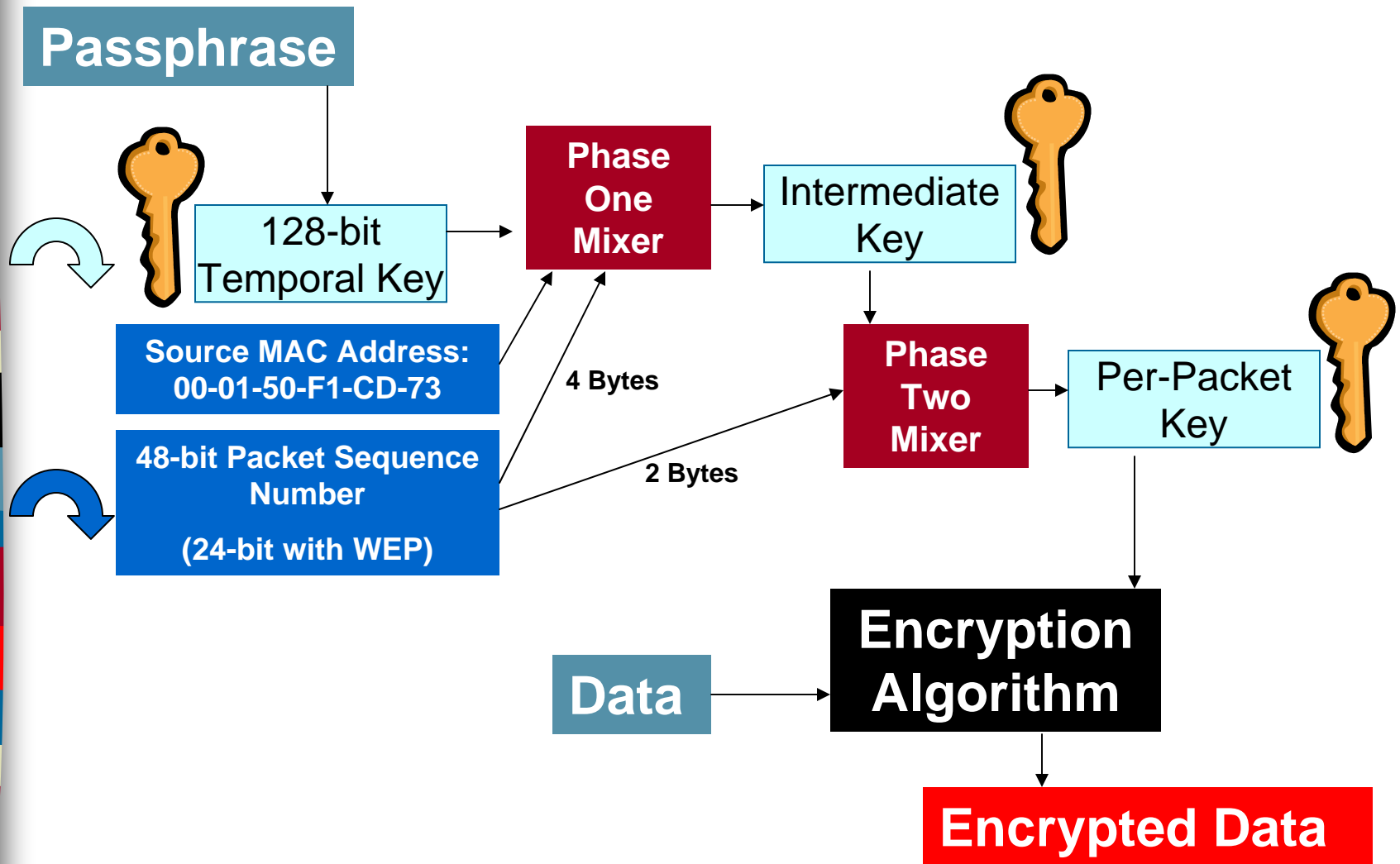
Entered once or updated by user if they feel like it.



# Per-Packet Keying

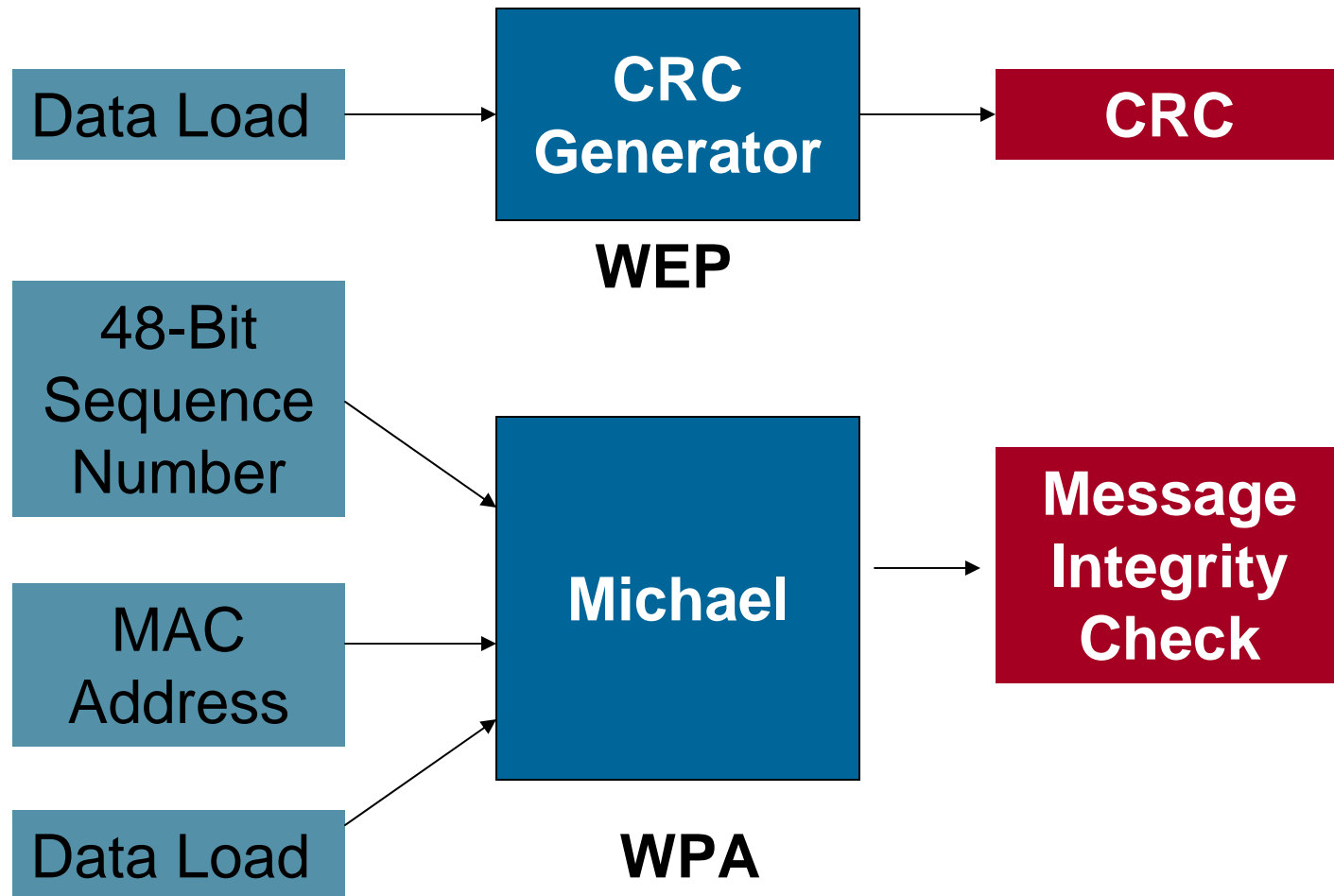
- Each packet is generated using a unique key
- Much more difficult to get from data back to the key
- Packet sequence number rollover
  - 24-bit sequence number with WEP would rollover leading to key re-use
  - 48-bit sequence number with WPA leads to new session key generation

# Per Packet Keying (cont.)



# Forgery Protection

## Step 1: Stronger Algorithm



# Forgery Protection

## Step 2: Forgery Detection

- Two forgeries in one second
- Radio assumes it is under attack.
- It deletes its session key, disassociates itself, then forces re-association.

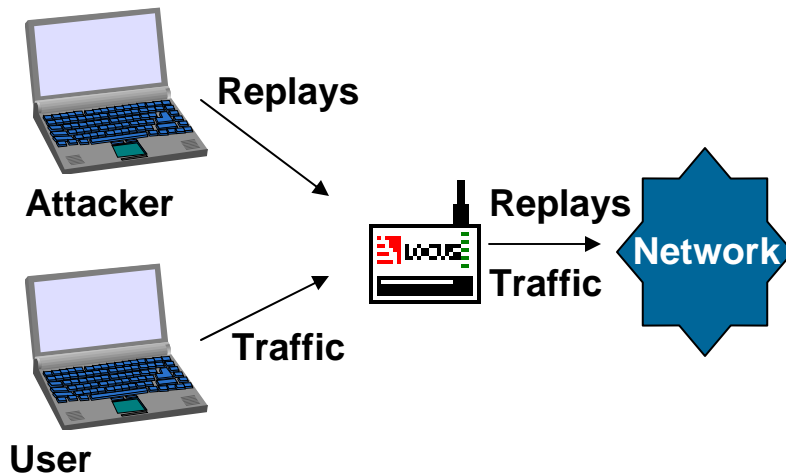


# Replay Prevention

Replays do not appear as a forgery

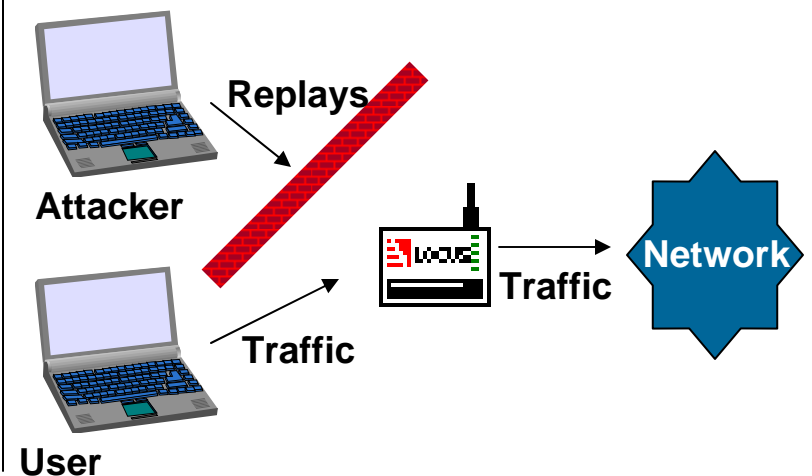
WEP

Overload the network by replaying a single packet



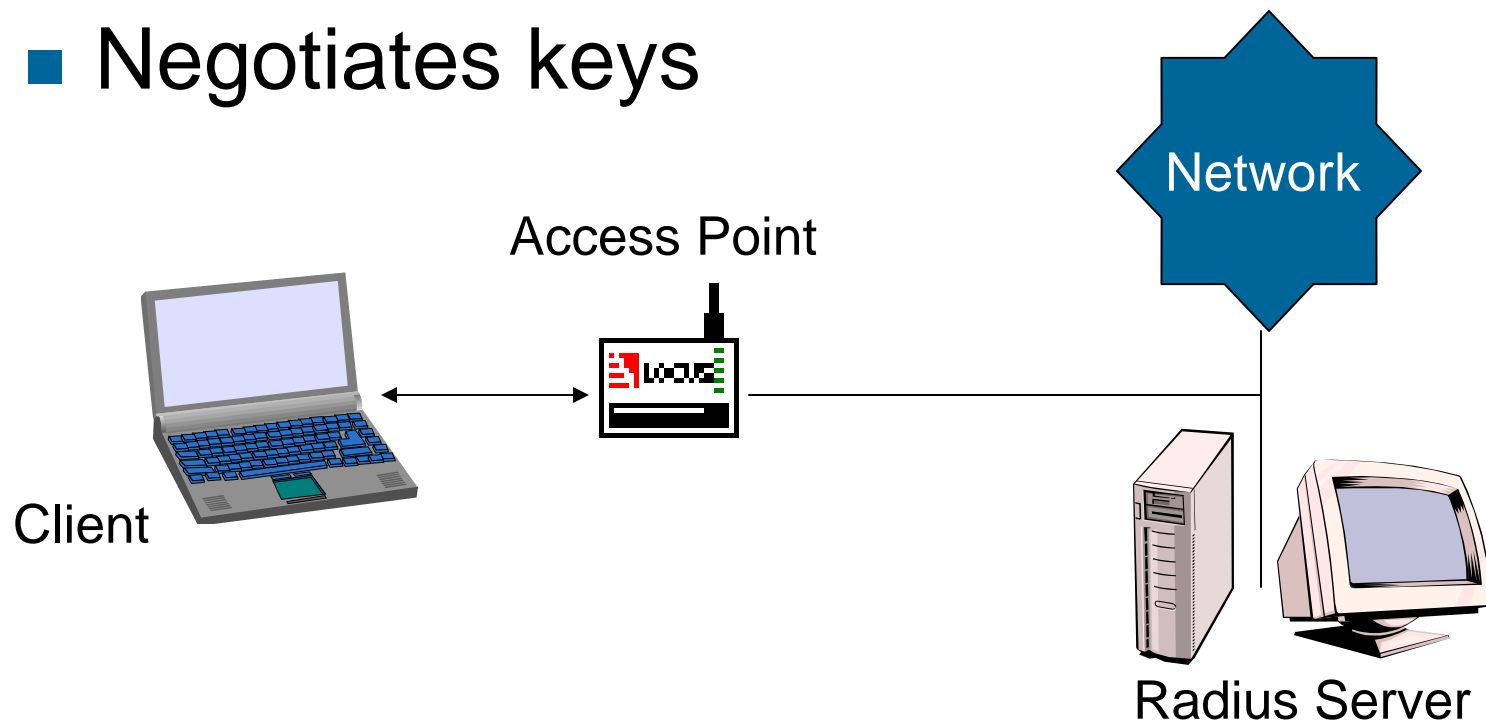
WPA

Network is protected  
IV must increment or  
packet is discarded



# RADIUS Server

- Authenticates clients before they are given access to the network
- Negotiates keys





# Need for a RADIUS Server

- Single point of key management
- Centralized administration
- Mix WEP/WPA amongst clients
- Seamless roaming without re-authentication
- Session time limits/time of day (user access policies)



# The Good Tool Used Properly

- Proper Authentication
- Proper Encryption
  - Packet Key Generation
  - System Key Distribution
  - Forgery Protection
  - Replay Prevention



# Scrutiny improves security

- Security by obscurity is a flawed approach.
- WPA has undergone great scrutiny by cryptographers.
- Scrutiny is the best way to provide security in an open protocol.

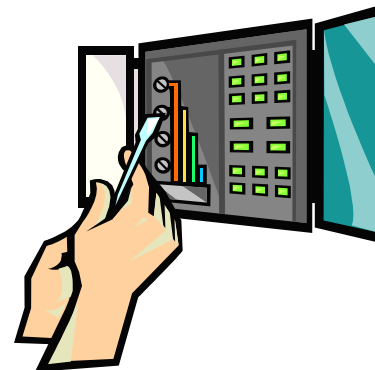
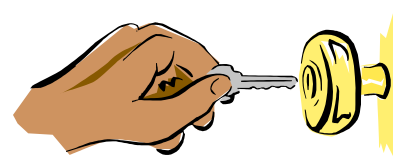


## More Security to Come

- 802.11i addresses immediate improvements as well as long-term improvements
  - ***Immediate*** improvements seen in WPA (TKIP Encryption) can run on current hardware
  - ***Long-term*** improvements include new encryption algorithm AES (Advanced Encryption Standard) which is more computationally intensive and requires new hardware

# Having the Best Security is Useless if...

- It isn't turned on
  - like having locks on your doors but not using them
- It is too complicated to understand
  - like having a security system for your house, but not knowing how to change the code





**Questions?**

**Thank you!**

Jim Weikert, Product Manager  
ProSoft Technology, Inc.  
Madison, WI