Wi-Fi Protected Access for Protection and Automation

Presented to: ACSAC-22 2006
13 December 2006
Dennis K. Holstein
on behalf of CIGRE B5.22
The good news and the bad news

- Who is CIGRE B5.22?
- What is Wi-Fi as defined by IEEE 802.11i?
- Let's get technical
  - WEP is not secure, so we now have WPA -> WPA2
  - Now we have 802.11i
  - Context is defined by limited-life keys
- What has this to do with Electric Power protection and automation?
  - Good question: we took a survey
  - What did we learn
- Defense in Depth
  - VLAN traffic separation
  - Radio planning to limit access
Who is CIGRE B5.22

- "CIGRE" is one of the leading worldwide Organizations on Electric Power Systems
- Study Committees are the main players of the technical activities – B5 is responsible for power system protection, substation control, automation, monitoring and recording
- B5.22 was commissioned to
  - Survey applications using Wi-Fi
  - Assess the mitigation of security vulnerabilities offered by IEEE 802.11i
  - Recommend design requirements and prioritized security levels
What is Wi-Fi

- Typically a Wi-Fi “adapter card” is embedded or inserted into a computer
- Wi-Fi provides simple wireless broadband access
- “Wi-Fi” is a brand name coined by the Wi-Fi Alliance
- Wi-Fi products must be designed using an industry standard, known as IEEE 802.11
  - Each subgroup of 802.11 is assigned a letter
  - “i” subgroup is responsible for developing an amendment to the 802.11 standard specifying security mechanisms for wireless networks
### What’s the difference between 802.11 a, b, g, & n

<table>
<thead>
<tr>
<th></th>
<th>Operating Band</th>
<th>Transfer Speed</th>
<th>Situation</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>5 GHz</td>
<td>54 Mbps</td>
<td>Line of sight – one direction only</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Never accepted in the market</td>
</tr>
<tr>
<td>802.11b</td>
<td>2.4 GHz</td>
<td>11 Mbps</td>
<td>Omni-directional</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4 GHz</td>
<td>54 Mbps</td>
<td>“b” and “g” are interoperable</td>
</tr>
<tr>
<td>802.11n</td>
<td>Solves the instability and interference issues with b &amp; g</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adds multiple input/multiple output (MIMO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Orthogonal frequency-division multiplexing (OFDM)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Uses several different receiver and transmitter antenna</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Increased data broadcast simultaneously</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
WEP is not secure, so we have WPA -> WPA2

- Original IEEE 802.11 did provide a security method - Wireless Equivalent Privacy (WEP)
  - Hacking software “AirSnort” published on the web
  - WEP security was instantly rendered useless
- Wi-Fi Protected Access (WPA) was the result
  - Better data encryption
  - Ability to authenticate users on large networks using a separate authentication service such as Remote Authentication Dial-In User Service
  - WPA use of Pre-Shared Keys (PSKs) – this is the problem
Now we have 802.11i

- Defines a new type of wireless network called
  - Robust Security Network (RSN)
  - Transitional Security Network (TSN)
- RSN and WEP systems can operate in parallel
- WPA and RSN share a common architecture and approach
  - WPA has a subset of capability focused specifically on one way to implement a network
  - RSN allows more flexibility in implementation
  - RSN supports the Advanced Encryption Standard (AES) cipher algorithm
Context is defined by limited-life keys

- Used to establish and maintain a security context between the wireless LAN devices - usually a mobile device and an access point
- This context is the “secret key” upon which security heavily relies
- RSN the security context is defined by the possession of limited-life keys – **temporal keys**
  - Creation of keys is done in real time as the security context is established, after authentication
  - Updated from time to time
  - Always destroyed when the security context is closed
- Authentication is based on some shared secret that cannot be created automatically
  - basis for all authentication methods is the entity to be authenticated possesses some special information in advance, which is called the **master key**
  - the master key is rarely, if ever, used directly; it is used to create temporal keys
Access control is critical

**Supplicant:** an entity that wants to have access

**Authenticator:** an entity that controls the access gate

**Authorizer:** An entity that decides whether the supplicant is to be admitted

PLC: Program Logic Controller – field device

PSTN: Public Switched Telephone Network
Access control – how it works

1. Authenticator is alerted by the supplicant
2. Supplicant identifies itself
3. Authenticator requests authorization from the authorizer
4. Authorizer indicates YES or NO
5. Authenticator allows or blocks access

Supplicant needs a “token” to prove it has been authorized

Key Material

Authentication Key

Wireless Network

Supplicant

Authenticator

Internet or other LAN resources

Authentication Server (RADIUS)

PLC

PSTN

ACSAC-22 2006 10
Three protocols used for WPA and RSN

- IEEE 802.1X – foundation for WPA and RSN
- EAP: Extensible Authentication Protocol (RFC2284)
- RADIUS: Remote Authentication Dial-in Service
  - Method of choice for WPA
  - Optional for RSN
The results from the survey are in

- The survey was sent to approximately 400 electric power utilities
  - serving at least 50,000 customers
  - having at least 20 electric power distribution and/or transmission substations
- More than 80 utilities from 32 countries participated

The situation today

- Little difference in current practices regarding Wi-Fi adoption and use
- Utility officials are not likely to use Wi-Fi at the present time
  - for sensitive mission-critical applications
  - such as protection and automation activities in electric power substations
Don’t despair
Look at the market opportunity

Two-thirds indicated that the utility could benefit from having a capability to obtain IED technical support at any time and regardless of location
More good news
Local access without entering the substation

- 36% could benefit - but had no plans to implement a solution
- 17% could benefit will implement a solution Q1 of 2008
- 44% need some education
Hard to reach IEDs are of interest

- 62% could benefit and already have the capability.
- 24% could benefit but had no plans to implement at this time.
- 13% said they could benefit and plan to implement a local access capability to reach IEDs by May of 2008.
- 1% said yes, but it's not in their plans at this time.
- 1% said no, it would not be a benefit for their utility.

24% could benefit but had no plans to implement at this time

13% said they could benefit and plan to implement a local access capability to reach IEDs by May of 2008.
The issue is security

- 43% - decision was based on the company’s security policy
- 22% - published articles discussing the risks of wireless use affected their decisions
- 10% - own experience, or other utility experiences, justified their position not to use wireless communications in the substation
- 19% - security did not have an effect on their decision not to use wireless approaches

71% indicated that security issues do have an effect on their decision not to use wireless communications in the substation
VLAN for traffic separation

- Adds a tag in all user originated frames {VLAN100 or VLAN200}
- IEEE 802.1x used to assign each user to a VLAN
- Radius server configures access points to support VLAN assignment
Antenna pattern shaping to limit access

Ideal omni-directional gain pattern

Sector panel shaped gain pattern
The answer to two questions

1. Are the security mechanisms adequate
   Yes, but utilities need to enforce two principles
   ● The principle of least privilege
   ● The principle of deny everything not-specified-allowed

2. Given the organizational complexities of power system operations can a system that relies on limited-life keys be efficiently managed
   ● Depends on the degree of complexity
   ● Closed self-contained operations – Yes
   ● Open federated operations – No
An effective security management scheme
Now for the quiz

- I use 802.11 – am I secure?
  - If you use WEP  NO
  - If you use WPA with passphrases  YES
  - If you use 802.11i  YES

- Does 802.11i address access control?  NO, Use 802.1x

- I’m a small utility – can I efficiently manage the keying material?
  - If you implement a Security Management Center  YES
  - If you use a trusted third-party security manager  YES

- I don’t want “stovepipe” solutions - does 802.11i fit with a comprehensive solution?
  
  Yes, because 802.11i implements a layered schema which is scaleable
What about me!

- I’m a large complex utility and I need to control access and use privileges
  - Between internal organizations
  - With business partners
  - With support organizations
  - With ISO, government and regulatory agencies

- **Good news**: 802.11i is secure – that’s not the problem
- **Good news**: If you can force a hierarchical management scheme, a well defined solution is available

- **Bad news**:
  - ISO, Government, and Regulatory agencies are the problem
  - You have a management nightmare on your hands
  - A federated, not a hierarchical, scheme is needed
  - A well understood federated management scheme does not exist
Thank you for your attention

Dennis K. Holstein
+1 562-176-4174
holsteindk@ieee.org