Comments on WAPI

Date: 2005-02-15

Authors:

Name	Company	Address	Phone	email
Clint Chaplin	Symbol Technologies	6480 Via Del Oro, San Jose, CA, USA 95119-1208	+1-408-528-2766	cchaplin@sj.symbol.com
Emily Qi	Intel Corporation	JF3-206, 2111 N.E. 25th Ave., Hillsboro, OR, USA 97124	+1-503-264-7799	emily.h.qi@intel.com
Henry Ptasinski	Broadcom	190 Matilda Place, Sunnyvale, CA, USA 94086	+1-408-543-3316	henryp@broadcom.com
Jesse Walker	Intel Corporation	JF3-206, 2111 N.E. 25th Ave, Hillsboro, OR, USA 97214	+1-503-712-1849	jesse.walker@intel.com
Sheung Li	Atheros Communications	529 Almanor Ave, Sunnyvale, CA, USA	+1-408-773-5295	sheung@atheros.com

Abstract

This document contains technical comments regarding JTC1/SC6's forwarding of the Chinese NB contribution (National Standard of China, GB15629.11) found in 6N12687 to the IEEE 802 (and specifically IEEE 802.11) for information.

Overview Statement

- GB15629.11 contains useful technology
- There are many issues to be resolved for successful integration of GB15629.11 into 802.11 and 8802-11
- We believe that cooperation between China's experts and the 802.11 Membership can successfully address all of these issues

Backward Compatibility Concerns

- **GB15629.11 omits provisions for backwards compatibility**
  - Its adoption would make all deployed implementations of 8802-11 non-compliant by removing all description of WEP.
  - While WEP may have many failings, continued support to facilitate migration is essential.
  - Removing WEP entirely represents an onerous economic burden on both users and vendors of 8802-11

Forward Compatibility Concerns

- **GB15629.11 does not consider forward compatibility**
  - It does not have any signaling mechanism to negotiate which cipher suite and authentication suite is used
  - This makes future enhancements more difficult
  - This blocks further innovation in the standard
- **GB15629.11's known incompatibilities include:**
  - IEEE Draft Std 802.11e
  - IEEE Draft Stds 802.11k, 802.11u, and 802.11w
  - IEEE Draft Std 802.11n
  - IEEE Draft Std 802.11r
  - IEEE Draft Std 802.11s
- **No mechanism will assure forward compatibility other than collaborating with IEEE 802.11 Working Group**

Interoperation Issues

- **Interoperation between equipment built for different jurisdictions prevented by GB15629.11**
  - Undesirable for a proposed international standard
- **In contrast, IEEE Std 802.11i provides an extensible security mechanism**
  - If a jurisdiction wishes to add new authentication algorithms and encryption algorithms (such as WAPI), they can do so within 802.11i framework
    - Without breaking interoperability with devices built for other jurisdictions
    - Without consent of IEEE 802.11 Working Group
    - And even without waiting for IEEE 802.11 Working Group to allocate one – use a vendor specific OUI

"Secret" Encryption Algorithm Concerns

- **GB15629.11 is incomplete, as it does not specify an encryption algorithm to use**
  - Implementation of the standard by all parties is not possible. Each vendor must be able to implement the encryption scheme
  - An international standard must specify all the algorithms needed for its implementation
- **In general almost no commercial market will trust or accept unknown ciphers**
- **It is infeasible to maintain the secrecy of any algorithm in mainstream commercial products**
  - Methods that effectively hinder reverse engineering of either hardware or software implementations too expensive for products in the consumer space
  - Private algorithms can only go in controlled products instead of commercial products to remain secret, e.g., military-only

Nations can maintain private algorithms, but only for non-standard modes of operation

Authentication Concerns (1)

- **GB15629.11 fails to consider global market requirements for authentication**
  - Different WLAN market segments require different authentication mechanisms
    - Enterprises plan to use EAP-TLS, PEAP, and TTLS, to leverage investment in RADIUS databases
    - 3GPP plans to use EAP-SIM, to leverage investment in GSM-SIM
    - China Mobile plans to use CAVE, to leverage its pre-existing authentication investment
    - Consumer electronics plans to use pre-shared keys, because homes do not have IT departments to manage on-line trusted third party servers

Authentication Concerns (2)

- **JTC1 already has an adopted digital certificate format—X.509. Why does it need another for 8802-11?**
  - No rationale given for GB15629.11 specific certificate formats
  - Certificate design known to be fraught with difficulty
    - GB15629.11 certificate is missing all the extensions that have been added to X.509 over the last decade to address obvious interoperability and operational problems
    - E.g., design does not consider ASU key expiry
    - E.g., design does not consider cross certification
    - E.g., design does not consider certificate chains longer than two certificates
- **Why is certificate design a WLAN specification issue?**
- **Why is back-end infrastructure a WLAN specification issue?**
  - It is true the back-end design must be considered to understand the system security, but it is not part of the WLAN

Other Technical Comments (1)

- **A STA can't distinguish a WAPI-enabled AP from a legacy AP**
- **An AP can’t distinguish a WAPI-enabled STA from a legacy STA**
- **As in 802.11i, authentication and key negotiation take place after association, leading to service disruption during AP-to-AP transition**
  - GB15629.11 is incompatible with 802.11r, so cannot utilize the fast roaming features developed by IEEE 802.11r

Security Issues

- **In an ad-hoc network, the same key is used by all STAs for all traffic. This is a security defect**
  - All STAs initialize the PN to the same value
  - Frames sent by different STAs will be protected with the same key and PN.
  - Since OFB is a stream cipher, this replicates WEP's known IV reuse defect
- **Uses plain CBC-MAC for MIC, a security defect**
  - CBC-MAC is not secure when used with variable length messages
    - See Bellare, Killian, and Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code," CRYPTO '94 Proceedings
  - Either reverse order of encryption and message integrity (this must be done with care to work), or else need a different message integrity code
- **Transmit and Receive addresses unprotected from forgery**

Abstract

This document contains technical comments regarding JTC1/SC6's forwarding of the Chinese NB contribution (National Standard of China, GB15629.11) found in 6N12687 to the IEEE 802 (and specifically IEEE 802.11) for information.

Overview Statement

- GB15629.11 contains useful technology
- There are many issues to be resolved for successful integration of GB15629.11 into 802.11 and 8802-11
- We believe that cooperation between China's experts and the 802.11 Membership can successfully address all of these issues

Backward Compatibility Concerns

- **GB15629.11 omits provisions for backwards compatibility**
  - Its adoption would make all deployed implementations of 8802-11 non-compliant by removing all description of WEP.
  - While WEP may have many failings, continued support to facilitate migration is essential.
  - Removing WEP entirely represents an onerous economic burden on both users and vendors of 8802-11

Forward Compatibility Concerns

- **GB15629.11 does not consider forward compatibility**
  - It does not have any signaling mechanism to negotiate which cipher suite and authentication suite is used
  - This makes future enhancements more difficult
  - This blocks further innovation in the standard
- **GB15629.11's known incompatibilities include:**
  - IEEE Draft Std 802.11e
  - IEEE Draft Stds 802.11k, 802.11u, and 802.11w
  - IEEE Draft Std 802.11n
  - IEEE Draft Std 802.11r
  - IEEE Draft Std 802.11s
- **No mechanism will assure forward compatibility other than collaborating with IEEE 802.11 Working Group**

Interoperation Issues

- **Interoperation between equipment built for different jurisdictions prevented by GB15629.11**
  - Undesirable for a proposed international standard
- **In contrast, IEEE Std 802.11i provides an extensible security mechanism**
  - If a jurisdiction wishes to add new authentication algorithms and encryption algorithms (such as WAPI), they can do so within 802.11i framework
    - Without breaking interoperability with devices built for other jurisdictions
    - Without consent of IEEE 802.11 Working Group
    - And even without waiting for IEEE 802.11 Working Group to allocate one – use a vendor specific OUI

"Secret" Encryption Algorithm Concerns

- **GB15629.11 is incomplete, as it does not specify an encryption algorithm to use**
  - Implementation of the standard by all parties is not possible. Each vendor must be able to implement the encryption scheme
  - An international standard must specify all the algorithms needed for its implementation
- **In general almost no commercial market will trust or accept unknown ciphers**
- **It is infeasible to maintain the secrecy of any algorithm in mainstream commercial products**
  - Methods that effectively hinder reverse engineering of either hardware or software implementations too expensive for products in the consumer space
  - Private algorithms can only go in controlled products instead of commercial products to remain secret, e.g., military-only

Nations can maintain private algorithms, but only for non-standard modes of operation

Authentication Concerns (1)

- **GB15629.11 fails to consider global market requirements for authentication**
  - Different WLAN market segments require different authentication mechanisms
    - Enterprises plan to use EAP-TLS, PEAP, and TTLS, to leverage investment in RADIUS databases
    - 3GPP plans to use EAP-SIM, to leverage investment in GSM-SIM
    - China Mobile plans to use CAVE, to leverage its pre-existing authentication investment
    - Consumer electronics plans to use pre-shared keys, because homes do not have IT departments to manage on-line trusted third party servers

Authentication Concerns (2)

- **JTC1 already has an adopted digital certificate format—X.509. Why does it need another for 8802-11?**
  - No rationale given for GB15629.11 specific certificate formats
  - Certificate design known to be fraught with difficulty
    - GB15629.11 certificate is missing all the extensions that have been added to X.509 over the last decade to address obvious interoperability and operational problems
    - E.g., design does not consider ASU key expiry
    - E.g., design does not consider cross certification
    - E.g., design does not consider certificate chains longer than two certificates
- **Why is certificate design a WLAN specification issue?**
- **Why is back-end infrastructure a WLAN specification issue?**
  - It is true the back-end design must be considered to understand the system security, but it is not part of the WLAN

Other Technical Comments (1)

- **A STA can't distinguish a WAPI-enabled AP from a legacy AP**
- **An AP can’t distinguish a WAPI-enabled STA from a legacy STA**
- **As in 802.11i, authentication and key negotiation take place after association, leading to service disruption during AP-to-AP transition**
  - GB15629.11 is incompatible with 802.11r, so cannot utilize the fast roaming features developed by IEEE 802.11r

Security Issues

- **In an ad-hoc network, the same key is used by all STAs for all traffic. This is a security defect**
  - All STAs initialize the PN to the same value
  - Frames sent by different STAs will be protected with the same key and PN.
  - Since OFB is a stream cipher, this replicates WEP's known IV reuse defect
- **Uses plain CBC-MAC for MIC, a security defect**
  - CBC-MAC is not secure when used with variable length messages
    - See Bellare, Killian, and Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code," CRYPTO '94 Proceedings
  - Either reverse order of encryption and message integrity (this must be done with care to work), or else need a different message integrity code
- **Transmit and Receive addresses unprotected from forgery**

Summary

- **Forward and backward compatibility have to be provided**
- **Interoperation issues needed to be resolved**
- **The following concerns should be addressed:**
  - "Secret" Encryption Algorithm Concerns
  - Performance and Cost Concerns
  - Authentication Concerns
- **A number of security issues in GB15629.11 must be addressed**
- **None of these issues are insurmountable if China's security experts work with the IEEE 802.11 Working Group to integrate GB15629.11 into ISO/IEC 8802-11 via IEEE 802.11 Working Group**