CE0973a - Issues in Network Security
9: WiFi Security, 802.1x

James A Sutherland

Abertay University

Monday, 7th March 2016

WiFi security and 802.1x

WiFi Security

- WEP, Wired Equivalent Privacy
- WPA, WiFi Protected Access
- WPA2, third time lucky
- WPS, WiFi Protected Setup

WiFi security and 802.1x

WiFi Security

- WEP, Wired Equivalent Privacy
- WPA, WiFi Protected Access
- WPA2, third time lucky
- WPS, WiFi Protected Setup

WiFi security and 802.1x

WiFi Security

- WEP, Wired Equivalent Privacy
- WPA, WiFi Protected Access
- WPA2, third time lucky
- WPS, WiFi Protected Setup

WiFi security and 802.1x

WiFi Security

- WEP, Wired Equivalent Privacy
- WPA, WiFi Protected Access
- WPA2, third time lucky
- WPS, WiFi Protected Setup

IEEE 802.11

Institute of Electrical and Electronics Engineers – standards body, 802.11 being the family of wireless networking standards. (Note also 802.3, the Ethernet family.)

Key standards:

Year	Standard	Frequency	Bandwidth
1999	a	5	54
1999	b	2.4	11
2003	g	2.4	54
2009	n	2.4/5	150
2013	ac	5	867
2012	ad	60	6912

WiFi starting point, 1999

- Back in 1999, first widespread wireless
- 11 Mbps in theory, about half in practice
- Crowded frequency: microwaves, other radio devices
- 14 channels (14 is Japan only, 12 and 13 not allowed in USA)
- Security: originally WEP

WiFi starting point, 1999

- Back in 1999, first widespread wireless
- 11 Mbps in theory, about half in practice
- Crowded frequency: microwaves, other radio devices
- 14 channels (14 is Japan only, 12 and 13 not allowed in USA)
- Security: originally WEP

WiFi starting point, 1999

- Back in 1999, first widespread wireless
- 11 Mbps in theory, about half in practice
- Crowded frequency: microwaves, other radio devices
- 14 channels (14 is Japan only, 12 and 13 not allowed in USA)
- Security: originally WEP

WiFi starting point, 1999

- Back in 1999, first widespread wireless
- 11 Mbps in theory, about half in practice
- Crowded frequency: microwaves, other radio devices
- 14 channels (14 is Japan only, 12 and 13 not allowed in USA)
- Security: originally WEP

WiFi starting point, 1999

- Back in 1999, first widespread wireless
- 11 Mbps in theory, about half in practice
- Crowded frequency: microwaves, other radio devices
- 14 channels (14 is Japan only, 12 and 13 not allowed in USA)
- Security: originally WEP

WEP: Wired Equivalent Privacy, 1997

- RC4 and CRC32
- 64 bit key – split into 24 bit IV, 40 bit key – export restriction
- Sniff enough traffic, passive attack yields key in 1 minute
- c 40k packets usually
- Prohibited by PCI DSS as of 2009 (grandfathered until 2010)
- Stream cipher with poor MAC, so vulnerable to bit-flipping attack

WEP: Wired Equivalent Privacy, 1997

- RC4 and CRC32
- 64 bit key – split into 24 bit IV, 40 bit key – export restriction
- Sniff enough traffic, passive attack yields key in 1 minute
- c 40k packets usually
- Prohibited by PCI DSS as of 2009 (grandfathered until 2010)
- Stream cipher with poor MAC, so vulnerable to bit-flipping attack

WEP: Wired Equivalent Privacy, 1997

- RC4 and CRC32
- 64 bit key – split into 24 bit IV, 40 bit key – export restriction
- Sniff enough traffic, passive attack yields key in 1 minute
- c 40k packets usually
- Prohibited by PCI DSS as of 2009 (grandfathered until 2010)
- Stream cipher with poor MAC, so vulnerable to bit-flipping attack

WEP: Wired Equivalent Privacy, 1997

- RC4 and CRC32
- 64 bit key – split into 24 bit IV, 40 bit key – export restriction
- Sniff enough traffic, passive attack yields key in 1 minute
- c 40k packets usually
- Prohibited by PCI DSS as of 2009 (grandfathered until 2010)
- Stream cipher with poor MAC, so vulnerable to bit-flipping attack

WEP: Wired Equivalent Privacy, 1997

- RC4 and CRC32
- 64 bit key – split into 24 bit IV, 40 bit key – export restriction
- Sniff enough traffic, passive attack yields key in 1 minute
- c 40k packets usually
- Prohibited by PCI DSS as of 2009 (grandfathered until 2010)
- Stream cipher with poor MAC, so vulnerable to bit-flipping attack

WEP: Wired Equivalent Privacy, 1997

- RC4 and CRC32
- 64 bit key – split into 24 bit IV, 40 bit key – export restriction
- Sniff enough traffic, passive attack yields key in 1 minute
- c 40k packets usually
- Prohibited by PCI DSS as of 2009 (grandfathered until 2010)
- Stream cipher with poor MAC, so vulnerable to bit-flipping attack

WPA: WiFi Protected Access, 2003

802.11i: WPA, then WPA2 – added:

- TKIP, Temporal Key Integrity Protocol – different key per packet[1]
- Replaced CRC with message integrity check "Michael"
- Defences! Two wrong MIC codes in 1 min – change TKIP key
- Mandatory CCMP: AES-based encryption (in all WiFi devices 2006-)
- Two variants: Personal (password), Enterprise (username+password)
- Enterprise uses 802.1x, Extensible Authentication Protocol

[1] TKIP is deprecated as of the 2012 revision

WPA: WiFi Protected Access, 2003

802.11i: WPA, then WPA2 – added:

- TKIP, Temporal Key Integrity Protocol – different key per packet[1]
- Replaced CRC with message integrity check “Michael”
- Defences! Two wrong MIC codes in 1 min – change TKIP key
- Mandatory CCMP: AES-based encryption (in all WiFi devices 2006-)
- Two variants: Personal (password), Enterprise (username+password)
- Enterprise uses 802.1x, Extensible Authentication Protocol

[1] TKIP is deprecated as of the 2012 revision

WPA: WiFi Protected Access, 2003

802.11i: WPA, then WPA2 – added:

- TKIP, Temporal Key Integrity Protocol – different key per packet[1]
- Replaced CRC with message integrity check "Michael"
- Defences! Two wrong MIC codes in 1 min – change TKIP key
- Mandatory CCMP: AES-based encryption (in all WiFi devices 2006-)
- Two variants: Personal (password), Enterprise (username+password)
- Enterprise uses 802.1x, Extensible Authentication Protocol

[1] TKIP is deprecated as of the 2012 revision

WPA: WiFi Protected Access, 2003

802.11i: WPA, then WPA2 – added:

- TKIP, Temporal Key Integrity Protocol – different key per packet[1]
- Replaced CRC with message integrity check “Michael”
- Defences! Two wrong MIC codes in 1 min – change TKIP key
- Mandatory CCMP: AES-based encryption (in all WiFi devices 2006-)
- Two variants: Personal (password), Enterprise (username+password)
- Enterprise uses 802.1x, Extensible Authentication Protocol

[1] TKIP is deprecated as of the 2012 revision

WPA: WiFi Protected Access, 2003

802.11i: WPA, then WPA2 – added:

- TKIP, Temporal Key Integrity Protocol – different key per packet[1]
- Replaced CRC with message integrity check "Michael"
- Defences! Two wrong MIC codes in 1 min – change TKIP key
- Mandatory CCMP: AES-based encryption (in all WiFi devices 2006-)
- Two variants: Personal (password), Enterprise (username+password)
- Enterprise uses 802.1x, Extensible Authentication Protocol

[1] TKIP is deprecated as of the 2012 revision

WPA: WiFi Protected Access, 2003

802.11i: WPA, then WPA2 – added:

- TKIP, Temporal Key Integrity Protocol – different key per packet[1]
- Replaced CRC with message integrity check "Michael"
- Defences! Two wrong MIC codes in 1 min – change TKIP key
- Mandatory CCMP: AES-based encryption (in all WiFi devices 2006-)
- Two variants: Personal (password), Enterprise (username+password)
- Enterprise uses 802.1x, Extensible Authentication Protocol

[1] TKIP is deprecated as of the 2012 revision

802.1x/EAP

EAP-TLS	Good old TLS, using client certificates for authentication
EAP-TTLS	Tunneling TLS, often used for non-certificate authentication (see also PEAP)
EAP-SIM	Uses SIM card for authentication
EAP-AKA	Authentication and Key Agreement using USIM[2]
PEAP	Protected EAP, wraps EAP traffic in a TLS tunnel

[2] SIM application which runs on a UICC, Universal Integrated Circuit Card

WPS: WiFi Protected Setup, 2006

- Simple ... but not very secure.
- 8 digit PIN, but in two halves
- Multiple effective brute-force attacks
- “Pixie Dust” attack: bad random numbers lead to 90 second compromise

WPS: WiFi Protected Setup, 2006

- Simple ... but not very secure.
- 8 digit PIN, but in two halves
- Multiple effective brute-force attacks
- "Pixie Dust" attack: bad random numbers lead to 90 second compromise

WPS: WiFi Protected Setup, 2006

- Simple ... but not very secure.
- 8 digit PIN, but in two halves
- Multiple effective brute-force attacks
- “Pixie Dust” attack: bad random numbers lead to 90 second compromise

WPS: WiFi Protected Setup, 2006

- Simple ... but not very secure.
- 8 digit PIN, but in two halves
- Multiple effective brute-force attacks
- “Pixie Dust” attack: bad random numbers lead to 90 second compromise

Lab Work

- Log in to eduroam
- Which standard is used?
- How is it secured?
- How does Eduroam identify the RADIUS server?
- Vulnerabilities
- Find Janet policies for Eduroam

Lab Work

- Log in to eduroam
- Which standard is used?
- How is it secured?
- How does Eduroam identify the RADIUS server?
- Vulnerabilities
- Find Janet policies for Eduroam

Lab Work

- Log in to eduroam
- Which standard is used?
- How is it secured?
- How does Eduroam identify the RADIUS server?
- Vulnerabilities
- Find Janet policies for Eduroam

Lab Work

- Log in to eduroam
- Which standard is used?
- How is it secured?
- How does Eduroam identify the RADIUS server?
- Vulnerabilities
- Find Janet policies for Eduroam

Lab Work

- Log in to eduroam
- Which standard is used?
- How is it secured?
- How does Eduroam identify the RADIUS server?
- Vulnerabilities
- Find Janet policies for Eduroam

Lab Work

- Log in to eduroam
- Which standard is used?
- How is it secured?
- How does Eduroam identify the RADIUS server?
- Vulnerabilities
- Find Janet policies for Eduroam