CORSO DI GESTIONE DELLE RETI DI TELECOMUNICAZIONI

LENST - LABORATORIO DI ELABORAZIONE NUMERICA DEI SEGNALI E TELEMATICA

Sicurezza del protocollo 802.11

Leonardo Maccari
maccari@lenst.det.unifi.it

queste slides sono scritte in LaTeX e distribuite con licenza
Creative Commons
http://creativecommons.org/licenses/by-nc-sa/2.0/

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Sommario

Descrizione di 802.11
- Funzionamento generale
- Wireless Equivalent Privacy

Sicurezza di 802.11
- Denial of service
- Attacchi sull'autenticazione
- Gestione delle chiavi
- Debolezza degli algoritmi

Protocollo 802.11i
- Introduzione

Introduzione alle reti 802.11

- Standard che definisce lo strato fisico e lo strato MAC di reti wireless con una portata inferiore al Km
- Hanno ottenuto un enorme successo commerciale
- Le versioni a/b/g soffrivano di grossi problemi di sicurezza
- La sicurezza diventa ancora più rilevante:
  - Allontanamento dal gestore
  - Nuove problematiche: reti ad-hoc
- Si introduce il protocollo 802.11i

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Introduzione alle reti 802.11

- Standard che definisce lo strato fisico e lo strato MAC di reti wireless con una portata inferiore al Km
- Hanno ottenuto un enorme successo commerciale
- Le versioni a/b/g soffrivano di grossi problemi di sicurezza
- La sicurezza diventa ancora più rilevante:
  - Allontanamento dal gestore
  - Nuove problematiche: reti ad-hoc
- Si introduce il protocollo 802.11i

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Introduzione alle reti 802.11

- Standard che definisce lo strato fisico e lo strato MAC di reti wireless con una portata inferiore al Km
- Hanno ottenuto un enorme successo commerciale
- Le versioni a/b/g soffrivano di grossi problemi di sicurezza
- La sicurezza diventa ancora più rilevante:
  - Allontanamento dal gestore
  - Nuove problematiche: reti ad-hoc
- Si introduce il protocollo 802.11i

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Introduzione alle reti 802.11

- Standard che definisce lo strato fisico e lo strato MAC di reti wireless con una portata inferiore al Km
- Hanno ottenuto un enorme successo commerciale
- Le versioni a/b/g soffrivano di grossi problemi di sicurezza
- La sicurezza diventa ancora più rilevante:
  - Allontanamento dal gestore
  - Nuove problematiche: reti ad-hoc
- Si introduce il protocollo 802.11i

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Introduzione alle reti 802.11

- Standard che definisce lo strato fisico e lo strato MAC di reti wireless con una portata inferiore al Km
- Hanno ottenuto un enorme successo commerciale
- Le versioni a/b/g soffrivano di grossi problemi di sicurezza
- La sicurezza diventa ancora più rilevante:
  - Allontanamento dal gestore
  - Nuove problematiche: reti ad-hoc
- Si introduce il protocollo 802.11i

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Introduzione alle reti 802.11

- Standard che definisce lo strato fisico e lo strato MAC di reti wireless con una portata inferiore al Km
- Hanno ottenuto un enorme successo commerciale
- Le versioni a/b/g soffrivano di grossi problemi di sicurezza
- La sicurezza diventa ancora più rilevante:
  - Allontanamento dal gestore
  - Nuove problematiche: reti ad-hoc
- Si introduce il protocollo 802.11i

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

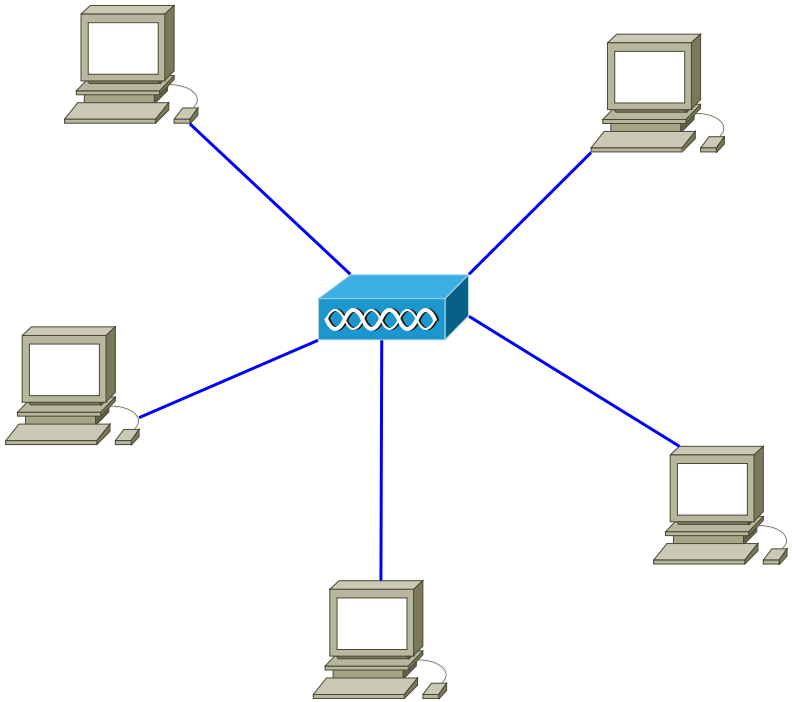
Introduzione alle reti 802.11

- Standard che definisce lo strato fisico e lo strato MAC di reti wireless con una portata inferiore al Km
- Hanno ottenuto un enorme successo commerciale
- Le versioni a/b/g soffrivano di grossi problemi di sicurezza
- La sicurezza diventa ancora più rilevante:
  - Allontanamento dal gestore
  - Nuove problematiche: reti ad-hoc
- Si introduce il protocollo 802.11i

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Reti 802.11a/b/g

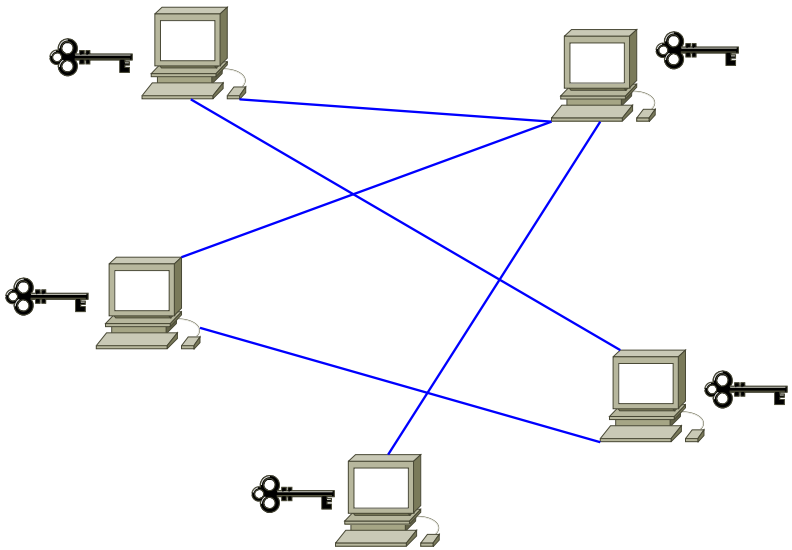


Modalità:

- Modello infrastructure (centralizzato)
- Modello ad-hoc (distribuito)
- Utilizzano il protocollo WEP per la sicurezza

Prestazioni

Reti 802.11a/b/g



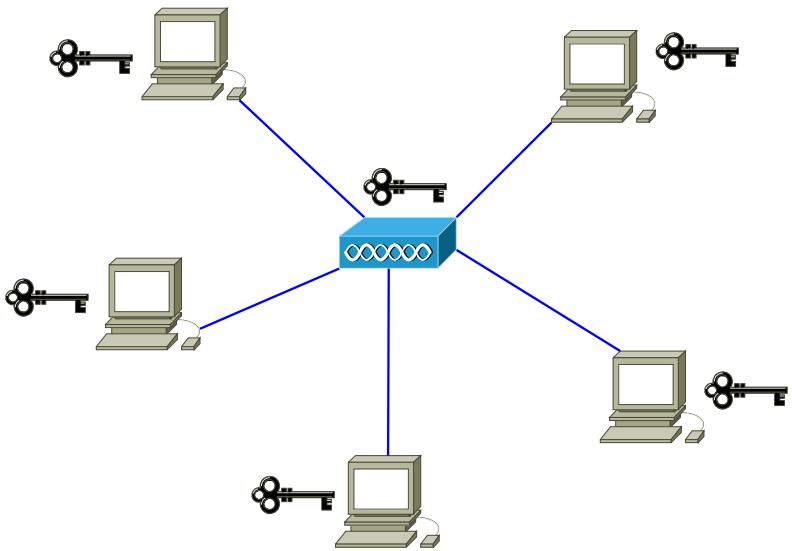
Modalità:

- Modello infrastructure (centralizzato)
- Modello ad-hoc (distribuito)
- Utilizzano il protocollo WEP per la sicurezza

Prestazioni

- dagli 11 ai 54 Mbps
- [illegible]

Reti 802.11a/b/g



Modalità:

- Modello infrastructure (centralizzato)
- Modello ad-hoc (distribuito)
- Utilizzano il protocollo WEP per la sicurezza

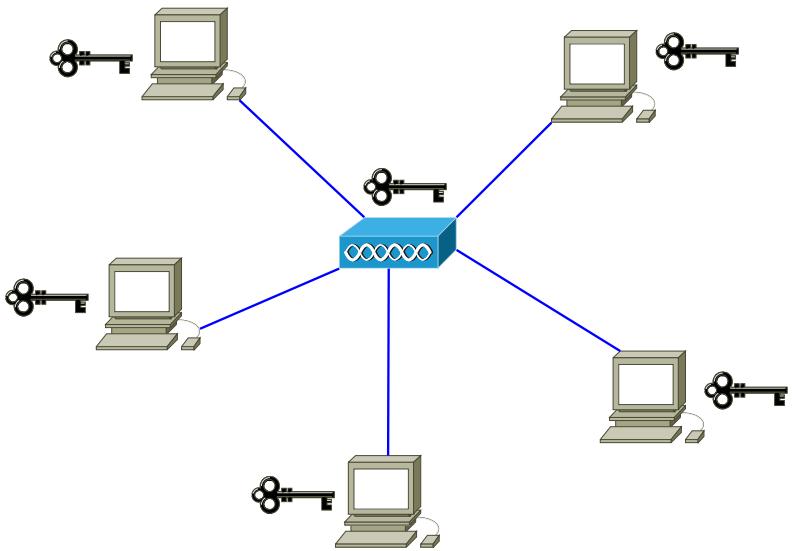
Prestazioni

- dagli 11 ai 54 Mbps
- raggio nell'ordine delle centinaia di metri

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Reti 802.11a/b/g



Modalità:

- Modello infrastructure (centralizzato)
- Modello ad-hoc (distribuito)
- Utilizzano il protocollo WEP per la sicurezza

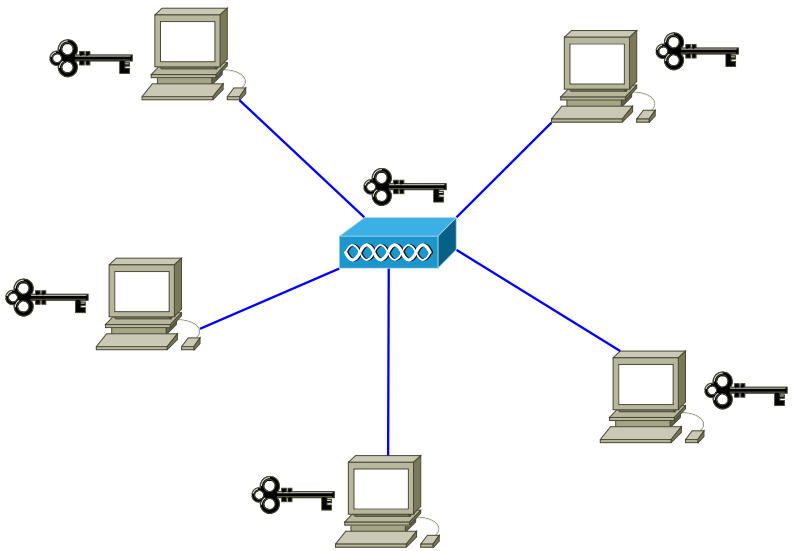
Prestazioni

- dagli 11 ai 54 Mbps
- raggio nell'ordine delle centinaia di metri

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Reti 802.11a/b/g



Modalità:

- Modello infrastructure (centralizzato)
- Modello ad-hoc (distribuito)
- Utilizzano il protocollo WEP per la sicurezza

Prestazioni

- dagli 11 ai 54 Mbps
- raggio nell'ordine delle centinaia di metri

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Wireless Equivalent Privacy

Specifiche

- Una unica chiave simmetrica condivisa tra tutte le macchine, utilizzata per l'autenticazione e la cifratura di pacchetti unicast e broadcast
- I pacchetti cifrati sono solo i pacchetti di dati e non quelli di controllo e di managment
- Per la cifratura di utilizza l'algoritmo di tipo streaming RC4

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Wireless Equivalent Privacy

Specifiche

- Una unica chiave simmetrica condivisa tra tutte le macchine, utilizzata per l'autenticazione e la cifratura di pacchetti unicast e broadcast
- I pacchetti cifrati sono solo i pacchetti di dati e non quelli di controllo e di managment
- Per la cifratura di utilizza l'algoritmo di tipo streaming RC4

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Wireless Equivalent Privacy

Specifiche

- Una unica chiave simmetrica condivisa tra tutte le macchine, utilizzata per l'autenticazione e la cifratura di pacchetti unicast e broadcast
- I pacchetti cifrati sono solo i pacchetti di dati e non quelli di controllo e di managment
- Per la cifratura di utilizza l'algoritmo di tipo streaming RC4

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

802.11: meccanismi di accesso alla rete

Autenticazione

Autenticazione di tipo *shared key*, il client si deve autenticare verso l'AP dimostrando di possedere la chiave segreta.

1. il client chiede di autenticarsi
2. AP risponde con un *challenge text*
3. Il client risponde con il *challenge text cifrato*

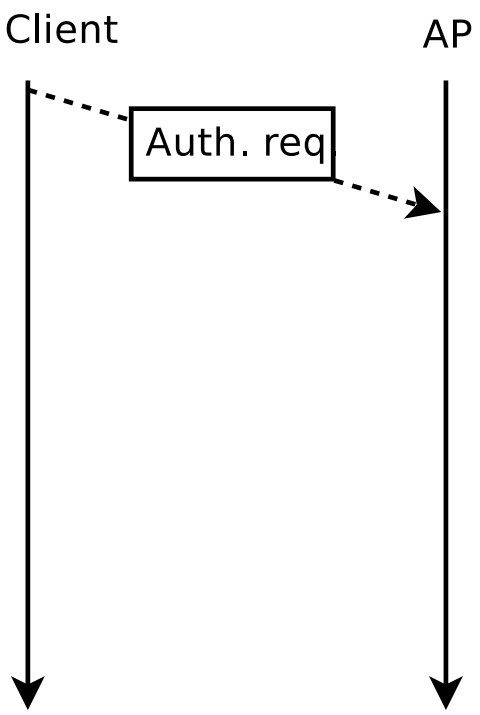
Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

802.11: meccanismi di accesso alla rete

Autenticazione

Autenticazione di tipo *shared key*, il client si deve autenticare verso l'AP dimostrando di possedere la chiave segreta.

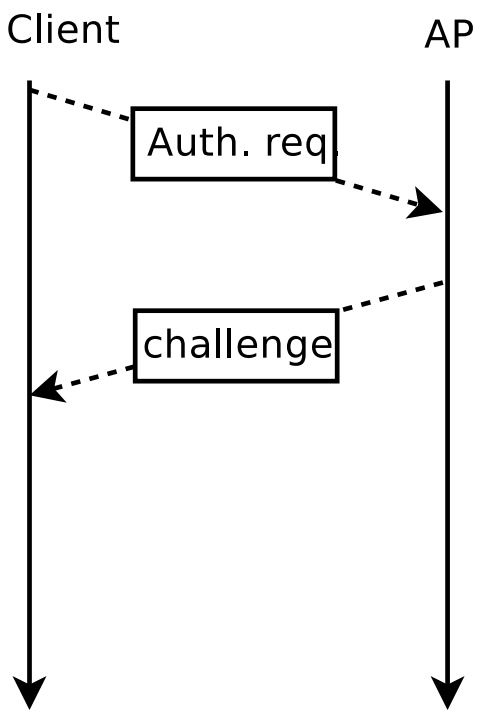


1. il client chiede di autenticarsi
2. AP risponde con un *challenge text*
3. Il client risponde con il *challenge text cifrato*

802.11: meccanismi di accesso alla rete

Autenticazione

Autenticazione di tipo *shared key*, il client si deve autenticare verso l'AP dimostrando di possedere la chiave segreta.

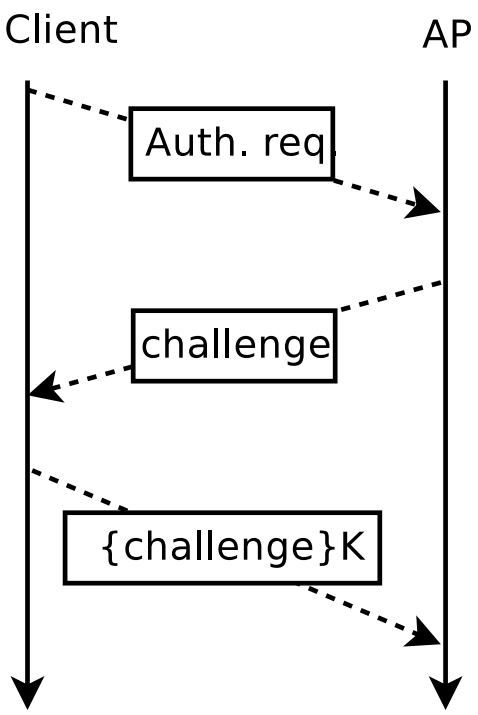


1. il client chiede di autenticarsi
2. AP risponde con un *challenge text*
3. Il client risponde con il *challenge text cifrato*

802.11: meccanismi di accesso alla rete

Autenticazione

Autenticazione di tipo *shared key*, il client si deve autenticare verso l'AP dimostrando di possedere la chiave segreta.



1. il client chiede di autenticarsi
2. AP risponde con un *challenge text*
3. Il client risponde con il *challenge text cifrato*

802.11: meccanismi di accesso alla rete

Associazione

Una volta autenticato il client deve notificare all'AP che vuole entrare nella rete.

1. il client chiede di associarsi
2. AP invia una conferma

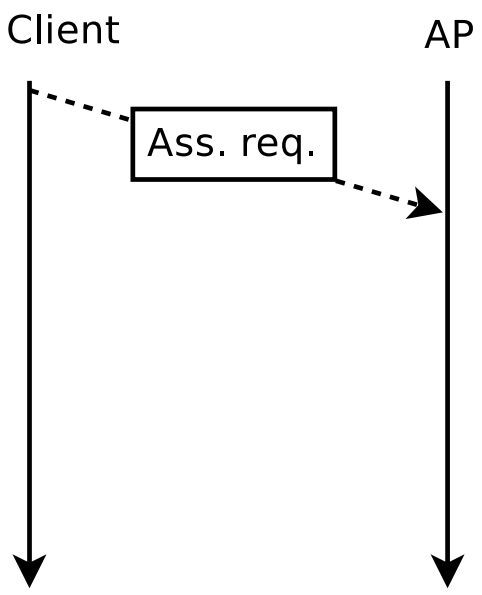
Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

802.11: meccanismi di accesso alla rete

Associazione

Una volta autenticato il client deve notificare all'AP che vuole entrare nella rete.

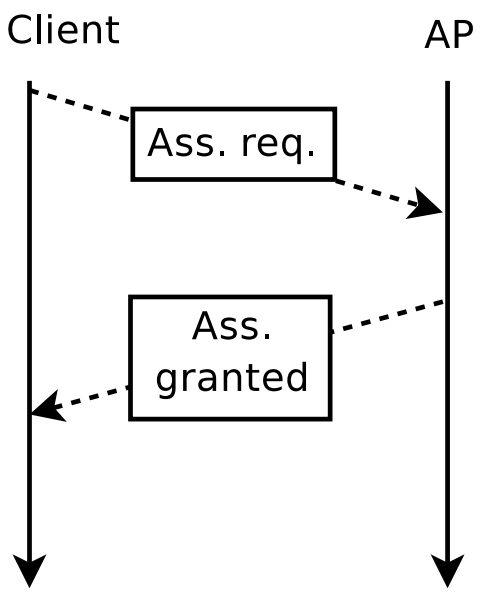


1. il client chiede di associarsi
2. AP invia una conferma

802.11: meccanismi di accesso alla rete

Associazione

Una volta autenticato il client deve notificare all'AP che vuole entrare nella rete.



1. il client chiede di associarsi
2. AP invia una conferma

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

802.11: meccanismi di uscita dalla rete

Deautenticazione e deassociazione

- per deautenticare il client il AP invia un messaggio di deautenticazione e il client deve ripetere l'autenticazione
- per deassociare un client l'AP invia un messaggio di deassociazione e il client deve ripetere l'associazione
- se riceve un messaggio di deautenticazione quando è anche associato il client deve ripetere entrambe le fasi

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

802.11: meccanismi di uscita dalla rete

Deautenticazione e deassociazione

- per deautenticare il client il AP invia un messaggio di deautenticazione e il client deve ripetere l'autenticazione
- per deassociare un client l'AP invia un messaggio di deassociazione e il client deve ripetere l'associazione
- se riceve un messaggio di deautenticazione quando è anche associato il client deve ripetere entrambe le fasi

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

802.11: meccanismi di uscita dalla rete

Deautenticazione e deassociazione

- per deautenticare il client il AP invia un messaggio di deautenticazione e il client deve ripetere l'autenticazione
- per deassociare un client l'AP invia un messaggio di deassociazione e il client deve ripetere l'associazione
- se riceve un messaggio di deautenticazione quando è anche associato il client deve ripetere entrambe le fasi

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

802.11: accesso al canale

- i client della LAN condividono lo stesso canale fisico
- in modalità infrastructure l'AP si comporta da centro stella, tutto il traffico viene inviato all'AP che lo ridirige ai client
- nell'intestazione di ogni pacchetto c'è un campo *Duration* in cui il client specifica un periodo di tempo in cui il canale è prenotato
- in quel periodo di tempo il canale non viene utilizzato da altri client

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

802.11: accesso al canale

- i client della LAN condividono lo stesso canale fisico
- in modalità infrastructure l'AP si comporta da centro stella, tutto il traffico viene inviato all'AP che lo ridirige ai client
- nell'intestazione di ogni pacchetto c'è un campo *Duration* in cui il client specifica un periodo di tempo in cui il canale è prenotato
- in quel periodo di tempo il canale non viene utilizzato da altri client

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

802.11: accesso al canale

- i client della LAN condividono lo stesso canale fisico
- in modalità infrastructure l'AP si comporta da centro stella, tutto il traffico viene inviato all'AP che lo ridirige ai client
- nell'intestazione di ogni pacchetto c'è un campo *Duration* in cui il client specifica un periodo di tempo in cui il canale è prenotato
- in quel periodo di tempo il canale non viene utilizzato da altri client

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

802.11: accesso al canale

- i client della LAN condividono lo stesso canale fisico
- in modalità infrastructure l'AP si comporta da centro stella, tutto il traffico viene inviato all'AP che lo ridirige ai client
- nell'intestazione di ogni pacchetto c'è un campo *Duration* in cui il client specifica un periodo di tempo in cui il canale è prenotato
- in quel periodo di tempo il canale non viene utilizzato da altri client

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Wirelss Equivalent Privacy

Con WEP viene chiamato l'insieme di procedure e di algoritmi utilizzati per garantire la sicurezza del protocollo. WEP prevede:

- Autenticazione delle macchine all'ingresso della rete
- Cifratura dei pacchetti: l'algoritmo utilizzato è RC4, un algoritmo di cifratura simmetrica di tipo *stream*
- Integrità dei pacchetti, prima di cifrare il pacchetto si aggiunge in coda un CRC-32

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Wirelss Equivalent Privacy

Con WEP viene chiamato l'insieme di procedure e di algoritmi utilizzati per garantire la sicurezza del protocollo. WEP prevede:

- Autenticazione delle macchine all'ingresso della rete
- Cifratura dei pacchetti: l'algoritmo utilizzato è RC4, un algoritmo di cifratura simmetrica di tipo *stream*
- Integrità dei pacchetti, prima di cifrare il pacchetto si aggiunge in coda un CRC-32

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Wirelss Equivalent Privacy

Con WEP viene chiamato l'insieme di procedure e di algoritmi utilizzati per garantire la sicurezza del protocollo. WEP prevede:

- Autenticazione delle macchine all'ingresso della rete
- Cifratura dei pacchetti: l'algoritmo utilizzato è RC4, un algoritmo di cifratura simmetrica di tipo *stream*
- Integrità dei pacchetti, prima di cifrare il pacchetto si aggiunge in coda un CRC-32

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Wirelss Equivalent Privacy

Con WEP viene chiamato l'insieme di procedure e di algoritmi utilizzati per garantire la sicurezza del protocollo. WEP prevede:

- Autenticazione delle macchine all'ingresso della rete
- Cifratura dei pacchetti: l'algoritmo utilizzato è RC4, un algoritmo di cifratura simmetrica di tipo *stream*
- Integrità dei pacchetti, prima di cifrare il pacchetto si aggiunge in coda un CRC-32

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Algoritmi di cifratura di tipo stream

Algoritmo

- A partire da un segreto condiviso e da un vettore d'inizializzazione (IV) si genera un vettore di lunghezza variabile di dati pseudocasuali (*keystream*)
- Si fa lo XOR logico tra il keystream e l'informazione che si vuole cifrare
- Gli algoritmi di tipo stream sono molto veloci e facili da implementare

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Algoritmi di cifratura di tipo stream

Algoritmo

- A partire da un segreto condiviso e da un vettore d'inizializzazione (IV) si genera un vettore di lunghezza variabile di dati pseudocasuali (*keystream*)
- Si fa lo XOR logico tra il keystream e l'informazione che si vuole cifrare
- Gli algoritmi di tipo stream sono molto veloci e facili da implementare

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Algoritmi di cifratura di tipo stream

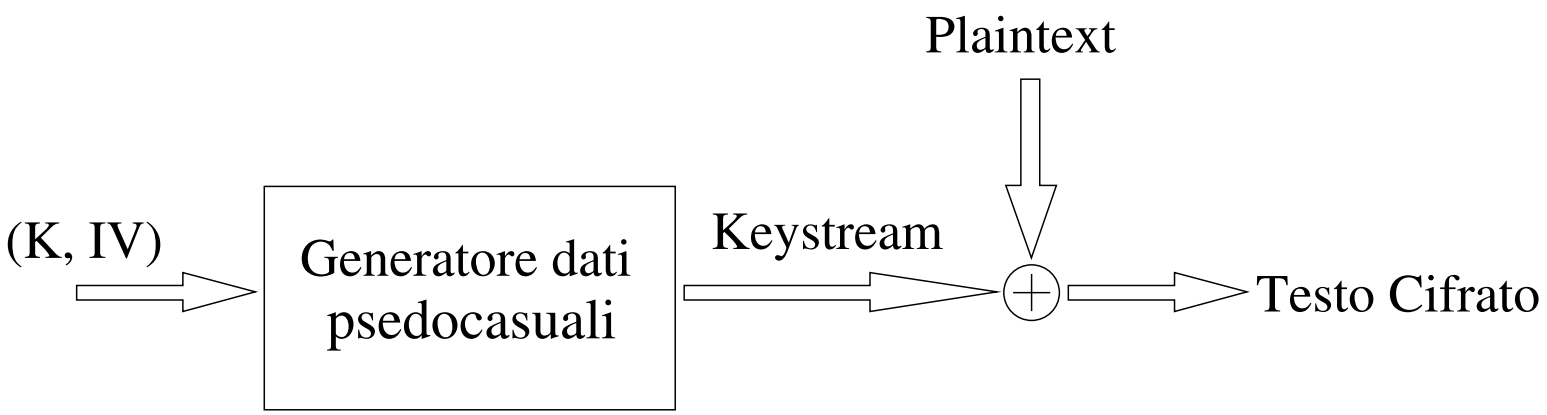
Algoritmo

- A partire da un segreto condiviso e da un vettore d'inizializzazione (IV) si genera un vettore di lunghezza variabile di dati pseudocasuali (*keystream*)
- Si fa lo XOR logico tra il keystream e l'informazione che si vuole cifrare
- Gli algoritmi di tipo stream sono molto veloci e facili da implementare

Leonardo Maccari,
maccari@lenst.det.unifi.

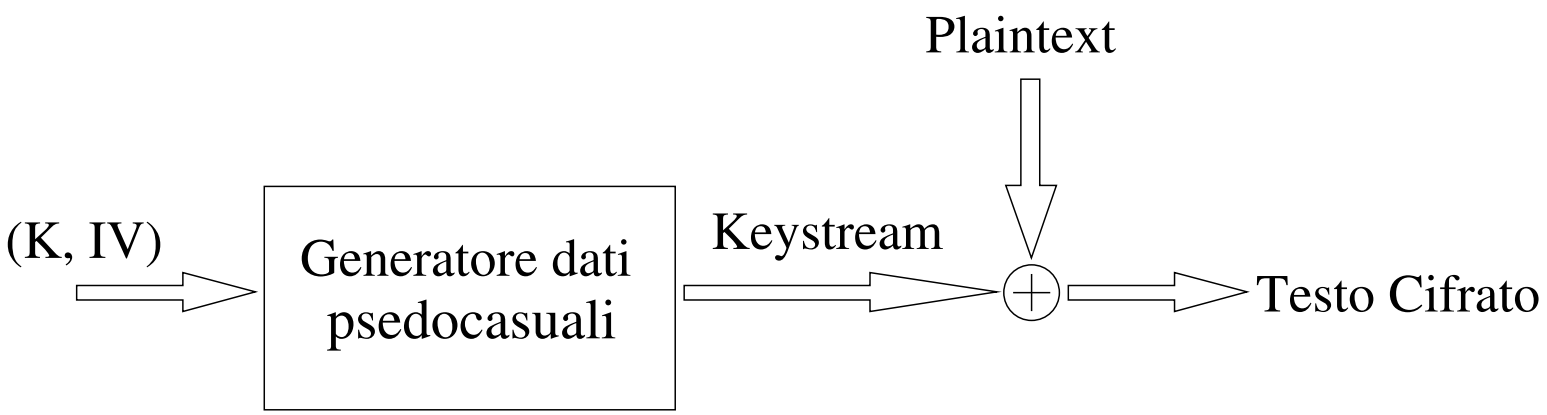
Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Cifratura di tipo stream



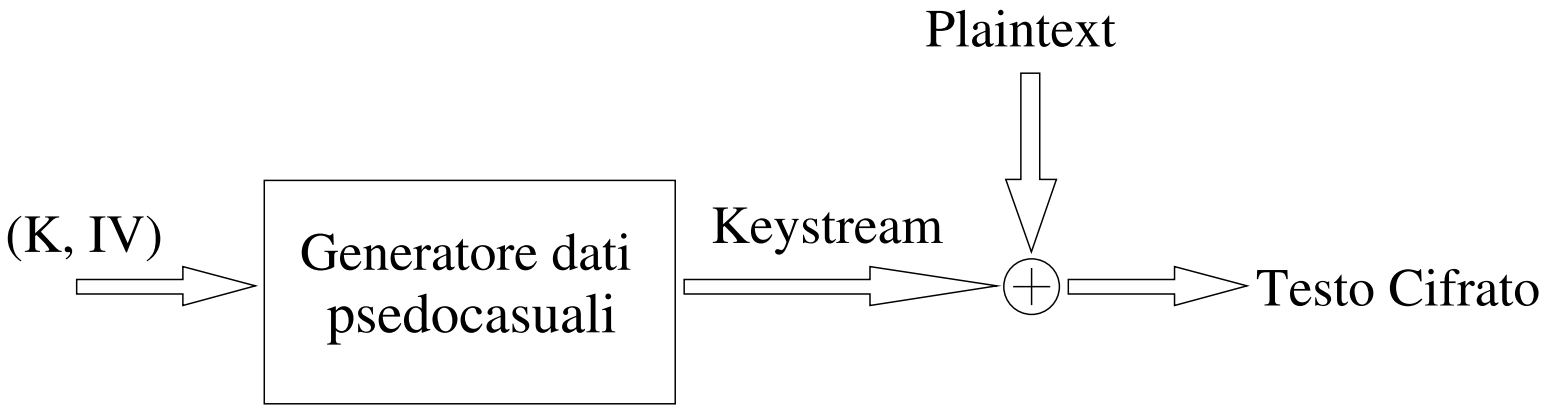
- Il periodo di ripetizione del keystream deve essere molto grande
- Lo stesso keystream non deve mai essere riutilizzato
  - $PlainT \oplus Keyst = CipherT \rightarrow CipherT \oplus Keyst = PlainT$
  - se si conosce uno dei testi cifrati con un certo keystream si ricava il keystream e quindi anche tutti gli altri testi cifrati con lo stesso keystream

Cifratura di tipo stream



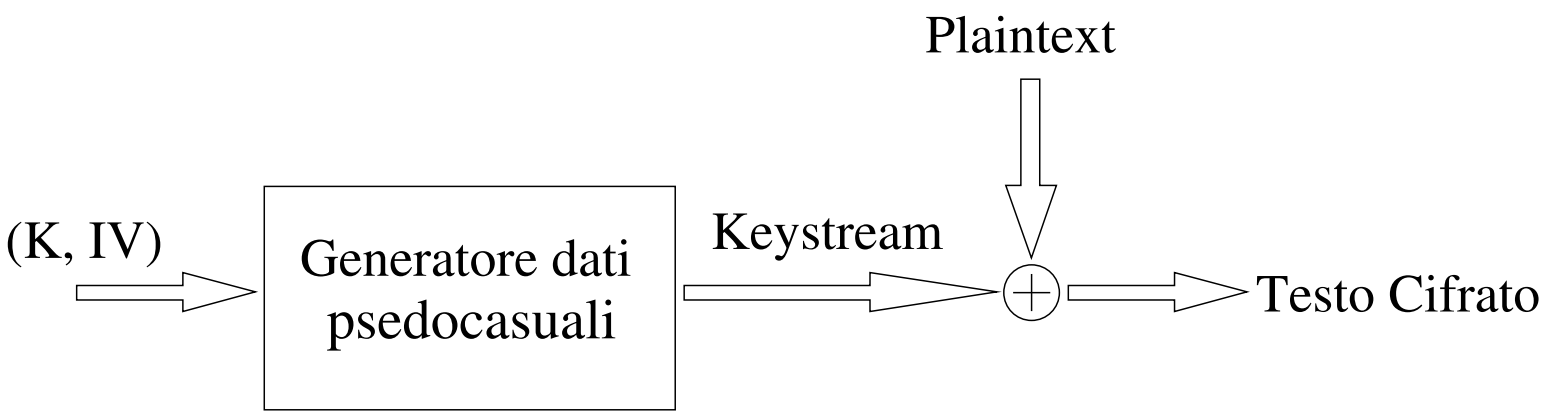
- Il periodo di ripetizione del keystream deve essere molto grande
- Lo stesso keystream non deve mai essere riutilizzato
  - $PlainT \oplus Keyst = CipherT \rightarrow CipherT \oplus Keyst = PlainT$
  - se si conosce uno dei testi cifrati con un certo keystream si ricava il keystream e quindi anche tutti gli altri testi cifrati con lo stesso keystream

Cifratura di tipo stream



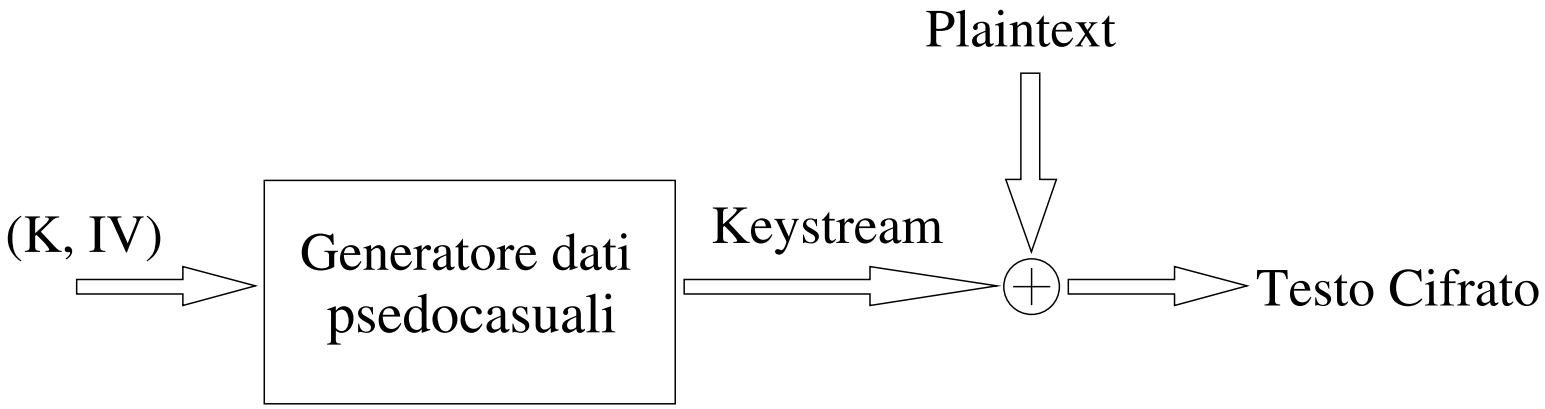
- Il periodo di ripetizione del keystream deve essere molto grande
- Lo stesso keystream non deve mai essere riutilizzato
  - $PlainT \oplus Keyst = CipherT \rightarrow CipherT \oplus Keyst = PlainT$
  - se si conosce uno dei testi cifrati con un certo keystream si ricava il keystream e quindi anche tutti gli altri testi cifrati con lo stesso keystream

Cifratura di tipo stream



- Il periodo di ripetizione del keystream deve essere molto grande
- Lo stesso keystream non deve mai essere riutilizzato
  - $PlainT \oplus Keyst = CipherT \rightarrow CipherT \oplus Keyst = PlainT$
  - se si conosce uno dei testi cifrati con un certo keystream si ricava il keystream e quindi anche tutti gli altri testi cifrati con lo stesso keystream

Cifratura di tipo stream



- Il periodo di ripetizione del keystream deve essere molto grande
- Lo stesso keystream non deve mai essere riutilizzato
  - $PlainT \oplus Keyst = CipherT \rightarrow CipherT \oplus Keyst = PlainT$
  - se si conosce uno dei testi cifrati con un certo keystream si ricava il keystream e quindi anche tutti gli altri testi cifrati con lo stesso keystream

Wirelss Equivalent Privacy

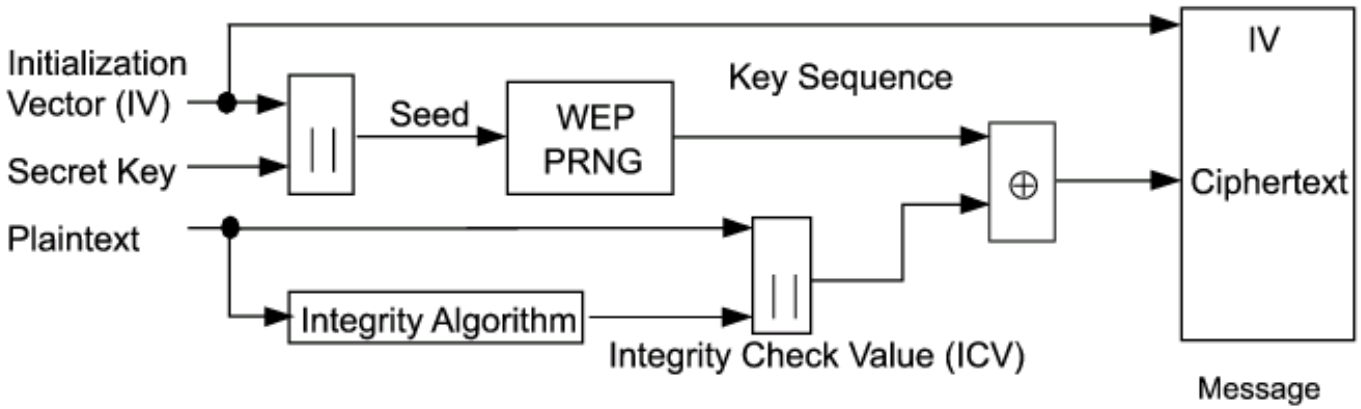


Figura: Processo di cifratura dei pacchetti 802.11

Wirelss Equivalent Privacy

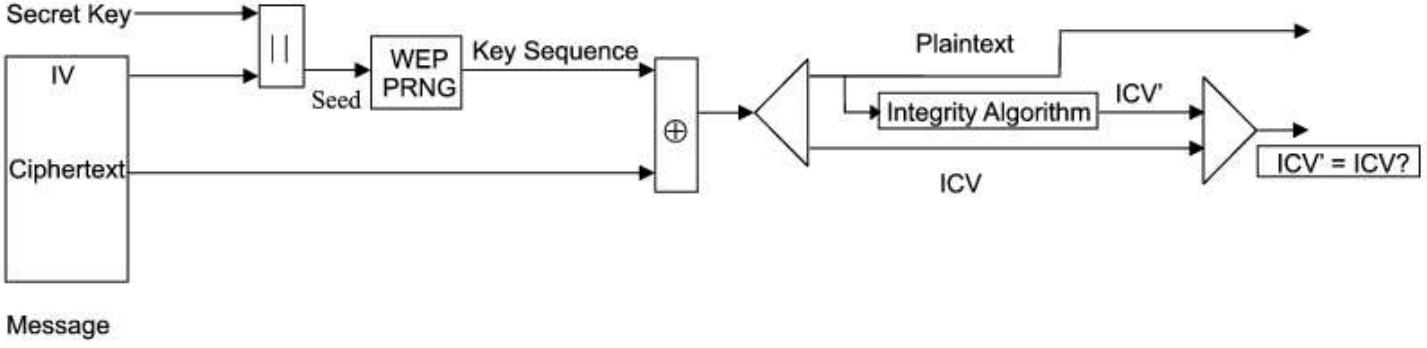


Figura: Processo di decifratura dei pacchetti 802.11

Tipi di pacchetti

802.11 definisce tre tipi di pacchetti:

- pacchetti di management: associazione, autenticazione, beacon . . .
- pacchetti di controllo: ack,rts, . . .
- pacchetti di dati

Pacchetti Cifrati:

- WEP cifra solo i pacchetti di dati

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Tipi di pacchetti

802.11 definisce tre tipi di pacchetti:

- pacchetti di management: associazione, autenticazione, beacon . . .
- pacchetti di controllo: ack,rts, . . .
- pacchetti di dati

Pacchetti Cifrati:

- WEP cifra solo i pacchetti di dati

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Tipi di pacchetti

802.11 definisce tre tipi di pacchetti:

- pacchetti di management: associazione, autenticazione, beacon . . .
- pacchetti di controllo: ack,rts, . . .
- pacchetti di dati

Pacchetti Cifrati:

- WEP cifra solo i pacchetti di dati

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Tipi di pacchetti

802.11 definisce tre tipi di pacchetti:

- pacchetti di management: associazione, autenticazione, beacon . . .
- pacchetti di controllo: ack,rts, . . .
- pacchetti di dati

Pacchetti Cifrati:

- WEP cifra solo i pacchetti di dati

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

DoS

Attacchi a livello fisico

- si può fare *jamming* su reti wireless
- difficilmente si riesce a oscurare un intero canale
- si può però impedire la corretta ricezione di almeno un bit provocando il fallimento del CRC e la ritrasmissione del pacchetto

Attacchi a livello MAC

Esistono una pletora di attacchi possibili:

- spoofing di pacchetti di deassociazione
- spoofing di pacchetti di deautenticazione
- flood di autenticazione su AP
- flood di prenotazione di canale

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

DoS

Attacchi a livello fisico

- si può fare *jamming* su reti wireless
- difficilmente si riesce a oscurare un intero canale
- si può però impedire la corretta ricezione di almeno un bit provocando il fallimento del CRC e la ritrasmissione del pacchetto

Attacchi a livello MAC

Esistono una pletora di attacchi possibili:

- spoofing di pacchetti di deassociazione
- spoofing di pacchetti di deautenticazione
- flood di autenticazione su AP
- flood di prenotazione di canale

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

DoS

Attacchi a livello fisico

- si può fare *jamming* su reti wireless
- difficilmente si riesce a oscurare un intero canale
- si può però impedire la corretta ricezione di almeno un bit provocando il fallimento del CRC e la ritrasmissione del pacchetto

Attacchi a livello MAC

Esistono una pletora di attacchi possibili:

- spoofing di pacchetti di deassociazione
- spoofing di pacchetti di deautenticazione
- flood di autenticazione su AP
- flood di prenotazione di canale

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

DoS

Attacchi a livello fisico

- si può fare *jamming* su reti wireless
- difficilmente si riesce a oscurare un intero canale
- si può però impedire la corretta ricezione di almeno un bit provocando il fallimento del CRC e la ritrasmissione del pacchetto

Attacchi a livello MAC

Esistono una pletora di attacchi possibili:

- spoofing di pacchetti di deassociazione
- spoofing di pacchetti di deautenticazione
- flood di autenticazione su AP
- flood di prenotazione di canale

DoS

Attacchi a livello fisico

- si può fare *jamming* su reti wireless
- difficilmente si riesce a oscurare un intero canale
- si può però impedire la corretta ricezione di almeno un bit provocando il fallimento del CRC e la ritrasmissione del pacchetto

Attacchi a livello MAC

Esistono una pletora di attacchi possibili:

- spoofing di pacchetti di deassociazione
- spoofing di pacchetti di deautenticazione
- flood di autenticazione su AP
- flood di prenotazione di canale

DoS

Attacchi a livello fisico

- si può fare *jamming* su reti wireless
- difficilmente si riesce a oscurare un intero canale
- si può però impedire la corretta ricezione di almeno un bit provocando il fallimento del CRC e la ritrasmissione del pacchetto

Attacchi a livello MAC

Esistono una pletora di attacchi possibili:

- spoofing di pacchetti di deassociazione
- spoofing di pacchetti di deautenticazione
- flood di autenticazione su AP
- flood di prenotazione di canale

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

DoS

Attacchi a livello fisico

- si può fare *jamming* su reti wireless
- difficilmente si riesce a oscurare un intero canale
- si può però impedire la corretta ricezione di almeno un bit provocando il fallimento del CRC e la ritrasmissione del pacchetto

Attacchi a livello MAC

Esistono una pletora di attacchi possibili:

- spoofing di pacchetti di deassociazione
- spoofing di pacchetti di deautenticazione
- flood di autenticazione su AP
- flood di prenotazione di canale

Attacchi sull'autenticazione shared key

Autenticazione shared key

L'autenticazione shared key è tragicamente insicura:

- Nel giro di pochi secondi passa lo stesso testo (128 byte) prima in chiaro e poi cifrato
  - l'attaccante può recuperare un frammento di keystream che può utilizzare per inviare pacchetti nella rete
- l'attaccante può effettuare un attacco di tipo reply anche senza conoscere la chiave, spacciandosi per l'AP
- l'attaccante può effettuare il famoso attacco dell'oracolo

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Attacchi sull'autenticazione shared key

Autenticazione shared key

L'autenticazione shared key è tragicamente insicura:

- Nel giro di pochi secondi passa lo stesso testo (128 byte) prima in chiaro e poi cifrato
  - l'attaccante può recuperare un frammento di keystream che può utilizzare per inviare pacchetti nella rete
- l'attaccante può effettuare un attacco di tipo reply anche senza conoscere la chiave, spacciandosi per l'AP
- l'attaccante può effettuare il famoso attacco dell'oracolo

Attacchi sull'autenticazione shared key

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Autenticazione shared key

L'autenticazione shared key è tragicamente insicura:

- Nel giro di pochi secondi passa lo stesso testo (128 byte) prima in chiaro e poi cifrato
  - l'attaccante può recuperare un frammento di keystream che può utilizzare per inviare pacchetti nella rete
- l'attaccante può effettuare un attacco di tipo reply anche senza conoscere la chiave, spacciandosi per l'AP
- l'attaccante può effettuare il famoso attacco dell'oracolo

Attacchi sull'autenticazione shared key

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Autenticazione shared key

L'autenticazione shared key è tragicamente insicura:

- Nel giro di pochi secondi passa lo stesso testo (128 byte) prima in chiaro e poi cifrato
  - l'attaccante può recuperare un frammento di keystream che può utilizzare per inviare pacchetti nella rete
- l'attaccante può effettuare un attacco di tipo reply anche senza conoscere la chiave, spacciandosi per l'AP
- l'attaccante può effettuare il famoso attacco dell'oracolo

Attacchi sull'autenticazione shared key

Attacco dell'oracolo

L'attaccante non conosce la chiave segreta ma vuole inviare un messaggio nella rete

- deautentica un client
- forgia un pacchetto con un challenge text contenente i dati che vuole inviare
- il client risponde restituendo il challenge text cifrato con un certo IV, ovvero il pacchetto valido per essere inviato lungo max 128 byte

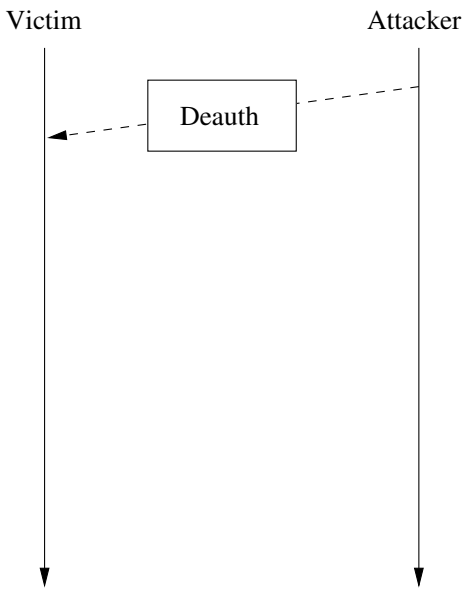
Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Attacchi sull'autenticazione shared key

Attacco dell'oracolo

L'attaccante non conosce la chiave segreta ma vuole inviare un messaggio nella rete

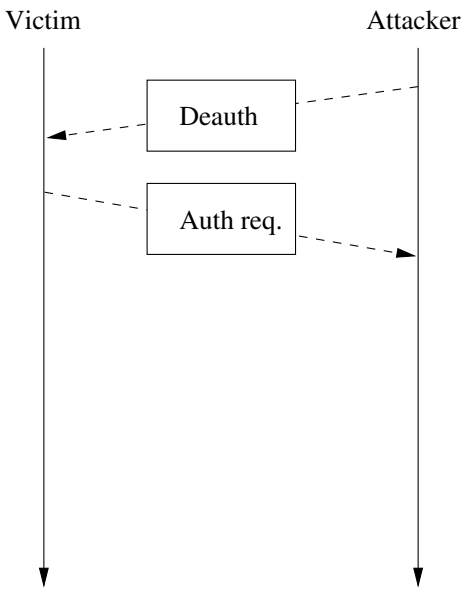


- deautentica un client
- forgia un pacchetto con un challenge text contenente i dati che vuole inviare
- il client risponde restituendo il challenge text cifrato con un certo IV, ovvero il pacchetto valido per essere inviato lungo max 128 byte

Attacchi sull'autenticazione shared key

Attacco dell'oracolo

L'attaccante non conosce la chiave segreta ma vuole inviare un messaggio nella rete

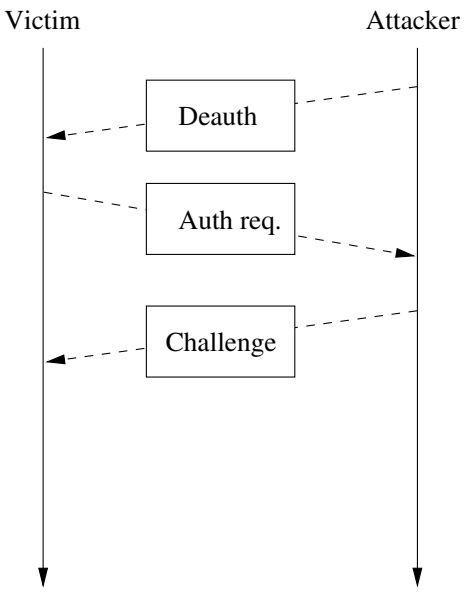


- deautentica un client
- forgia un pacchetto con un challenge text contenente i dati che vuole inviare
- il client risponde restituendo il challenge text cifrato con un certo IV, ovvero il pacchetto valido per essere inviato lungo max 128 byte

Attacchi sull'autenticazione shared key

Attacco dell'oracolo

L'attaccante non conosce la chiave segreta ma vuole inviare un messaggio nella rete

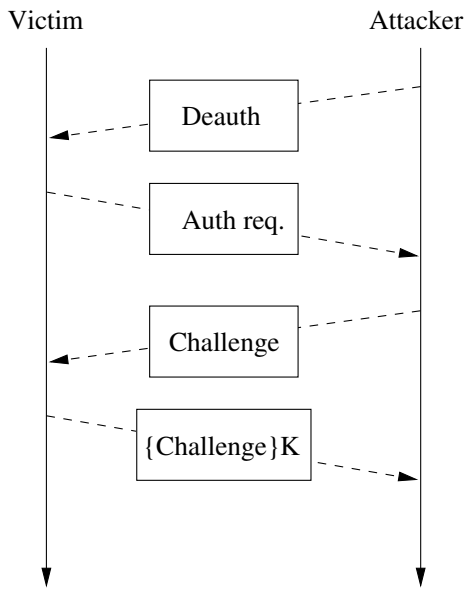


- deautentica un client
- forgia un pacchetto con un challenge text contenente i dati che vuole inviare
- il client risponde restituendo il challenge text cifrato con un certo IV, ovvero il pacchetto valido per essere inviato lungo max 128 byte

Attacchi sull'autenticazione shared key

Attacco dell'oracolo

L'attaccante non conosce la chiave segreta ma vuole inviare un messaggio nella rete



- deautentica un client
- forgia un pacchetto con un challenge text contenente i dati che vuole inviare
- il client risponde restituendo il challenge text cifrato con un certo IV, ovvero il pacchetto valido per essere inviato lungo max 128 byte

Attacchi sull'autenticazione shared key

Autenticazione dell'AP

L'attaccante vuole fare un attacco di tipo man in the middle verso un client

- deautentica un client
- forgia un pacchetto di autenticazione falso, con lo stesso ESSID dell'AP ma con WEP disattivato
- il client risponde facendo un'autenticazione open system, ovvero nessuna autenticazione
- da quel momento il client e' convinto di essere connesso all'AP giusto, ma comunica in chiaro

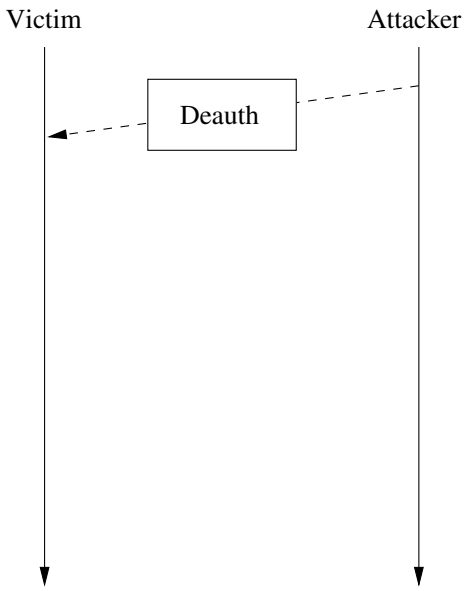
Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Attacchi sull'autenticazione shared key

Autenticazione dell'AP

L'attaccante vuole fare un attacco di tipo man in the middle verso un client

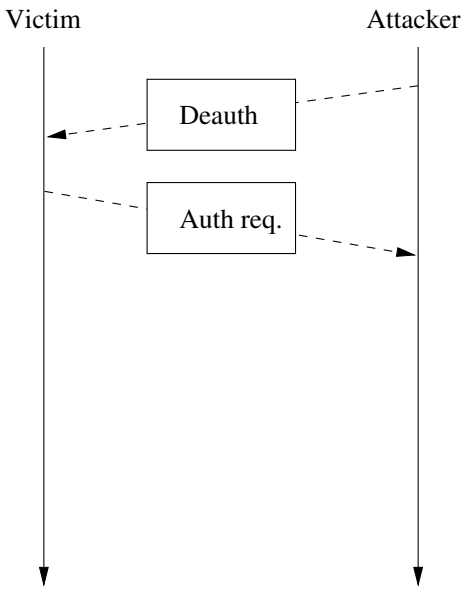


- deautentica un client
- forgia un pacchetto di autenticazione falso, con lo stesso ESSID dell'AP ma con WEP disattivato
- il client risponde facendo un'autenticazione open system, ovvero nessuna autenticazione
- da quel momento il client e' convinto di essere connesso all'AP giusto, ma comunica in chiaro

Attacchi sull'autenticazione shared key

Autenticazione dell'AP

L'attaccante vuole fare un attacco di tipo man in the middle verso un client

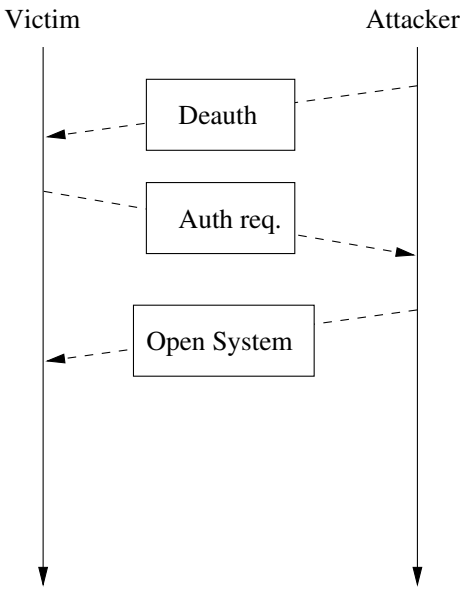


- deautentica un client
- forgia un pacchetto di autenticazione falso, con lo stesso ESSID dell'AP ma con WEP disattivato
- il client risponde facendo un'autenticazione open system, ovvero nessuna autenticazione
- da quel momento il client e' convinto di essere connesso all'AP giusto, ma comunica in chiaro

Attacchi sull'autenticazione shared key

Autenticazione dell'AP

L'attaccante vuole fare un attacco di tipo man in the middle verso un client

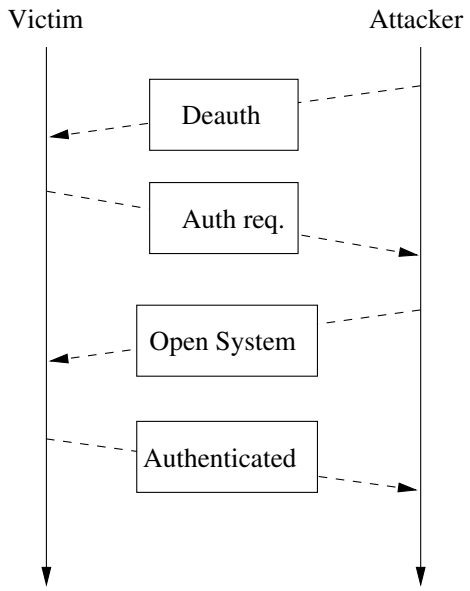


- deautentica un client
- forgia un pacchetto di autenticazione falso, con lo stesso ESSID dell'AP ma con WEP disattivato
- il client risponde facendo un'autenticazione open system, ovvero nessuna autenticazione
- da quel momento il client e' convinto di essere connesso all'AP giusto, ma comunica in chiaro

Attacchi sull'autenticazione shared key

Autenticazione dell'AP

L'attaccante vuole fare un attacco di tipo man in the middle verso un client

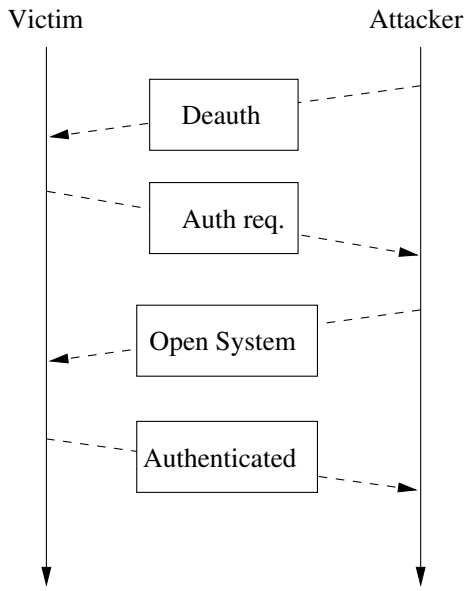


- deautentica un client
- forgia un pacchetto di autenticazione falso, con lo stesso ESSID dell'AP ma con WEP disattivato
- il client risponde facendo un'autenticazione open system, ovvero nessuna autenticazione
- da quel momento il client e' convinto di essere connesso all'AP giusto, ma comunica in chiaro

Attacchi sull'autenticazione shared key

Autenticazione dell'AP

L'attaccante vuole fare un attacco di tipo man in the middle verso un client



- deautentica un client
- forgia un pacchetto di autenticazione falso, con lo stesso ESSID dell'AP ma con WEP disattivato
- il client risponde facendo un'autenticazione open system, ovvero nessuna autenticazione
- da quel momento il client e' convinto di essere connesso all'AP giusto, ma comunica in chiaro

Attacchi sull'autenticazione shared key

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Autenticazione dell'AP

Questi attacchi sono possibili perche' l'autenticazione shared key, oltre ad essere male implementata porta un enorme errore di progetto:

- l'AP non si autentica con il client
- quindi chiunque si può fingere AP se conosce la chiave, ma anche se non la conosce può fingersi AP per certe operazioni

Attacchi sull'autenticazione shared key

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Autenticazione dell'AP

Questi attacchi sono possibili perche' l'autenticazione shared key, oltre ad essere male implementata porta un enorme errore di progetto:

- l'AP non si autentica con il client
- quindi chiunque si può fingere AP se conosce la chiave, ma anche se non la conosce può fingersi AP per certe operazioni

Attacchi sull'autenticazione shared key

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Autenticazione dell'AP

Questi attacchi sono possibili perche' l'autenticazione shared key, oltre ad essere male implementata porta un enorme errore di progetto:

- l'AP non si autentica con il client
- quindi chiunque si può fingere AP se conosce la chiave, ma anche se non la conosce può fingersi AP per certe operazioni

La gestione delle chiavi ...

...semplicemente non esiste.

Chiave WEP

Esiste una unica chiave condivisa da tutti i client, fissa, senza meccanismi automatici per cambiarla utilizzata per l'autenticazione e per la cifratura.

- ogni client può intercettare le comunicazioni degli altri client, che è pericoloso in ambienti in cui i client non sono fidati (hotspot)
- se la chiave viene compromessa non esiste un modo automatico per cambiarla (*rekey*) ma bisogna cambiarla a mano su tutti i client

Ma, penserete, la chiave *non* si può rompere, vero? ...vediamo.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

La gestione delle chiavi ...

...semplicemente non esiste.

Chiave WEP

Esiste una unica chiave condivisa da tutti i client, fissa, senza meccanismi automatici per cambiarla utilizzata per l'autenticazione e per la cifratura.

- ogni client può intercettare le comunicazioni degli altri client, che è pericoloso in ambienti in cui i client non sono fidati (hotspot)
- se la chiave viene compromessa non esiste un modo automatico per cambiarla (*rekey*) ma bisogna cambiarla a mano su tutti i client

Ma, penserete, la chiave *non* si può rompere, vero? ...vediamo.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

La gestione delle chiavi ...

...semplicemente non esiste.

Chiave WEP

Esiste una unica chiave condivisa da tutti i client, fissa, senza meccanismi automatici per cambiarla utilizzata per l'autenticazione e per la cifratura.

- ogni client può intercettare le comunicazioni degli altri client, che è pericoloso in ambienti in cui i client non sono fidati (hotspot)
- se la chiave viene compromessa non esiste un modo automatico per cambiarla (*rekey*) ma bisogna cambiarla a mano su tutti i client

Ma, penserete, la chiave *non* si può rompere, vero? ...vediamo.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

La gestione delle chiavi ...

...semplicemente non esiste.

Chiave WEP

Esiste una unica chiave condivisa da tutti i client, fissa, senza meccanismi automatici per cambiarla utilizzata per l'autenticazione e per la cifratura.

- ogni client può intercettare le comunicazioni degli altri client, che è pericoloso in ambienti in cui i client non sono fidati (hotspot)
- se la chiave viene compromessa non esiste un modo automatico per cambiarla (*rekey*) ma bisogna cambiarla a mano su tutti i client

Ma, penserete, la chiave *non* si può rompere, vero? ...vediamo.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

La gestione delle chiavi ...

...semplicemente non esiste.

Chiave WEP

Esiste una unica chiave condivisa da tutti i client, fissa, senza meccanismi automatici per cambiarla utilizzata per l'autenticazione e per la cifratura.

- ogni client può intercettare le comunicazioni degli altri client, che è pericoloso in ambienti in cui i client non sono fidati (hotspot)
- se la chiave viene compromessa non esiste un modo automatico per cambiarla (*rekey*) ma bisogna cambiarla a mano su tutti i client

Ma, penserete, la chiave *non* si può rompere, vero? ...vediamo.

La gestione delle chiavi ...

...semplicemente non esiste.

Chiave WEP

Esiste una unica chiave condivisa da tutti i client, fissa, senza meccanismi automatici per cambiarla utilizzata per l'autenticazione e per la cifratura.

- ogni client può intercettare le comunicazioni degli altri client, che è pericoloso in ambienti in cui i client non sono fidati (hotspot)
- se la chiave viene compromessa non esiste un modo automatico per cambiarla (*rekey*) ma bisogna cambiarla a mano su tutti i client

Ma, penserete, la chiave *non* si può rompere, vero? ...vediamo.

IV corto

- il keystream non si deve ripetere, ma la chiave è fissa, quindi il keystream cambia se cambia IV, quanto è lungo IV?
  - 24 bit → 16.777.216 di IV diversi, uno per pacchetto
  - ogni pacchetto tipicamente è lungo 1500 byte, in totale perchè IV si ripeta devono passare circa 25G di dati, che su una rete con 30Mbit/s di banda si ottengono in circa due ore.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

IV corto

- il keystream non si deve ripetere, ma la chiave è fissa, quindi il keystream cambia se cambia IV, quanto è lungo IV?
  - 24 bit → 16.777.216 di IV diversi, uno per pacchetto
  - ogni pacchetto tipicamente è lungo 1500 byte, in totale perchè IV si ripeta devono passare circa 25G di dati, che su una rete con 30Mbit/s di banda si ottengono in circa due ore.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

IV corto

- il keystream non si deve ripetere, ma la chiave è fissa, quindi il keystream cambia se cambia IV, quanto è lungo IV?
  - 24 bit $\rightarrow$ 16.777.216 di IV diversi, uno per pacchetto
  - ogni pacchetto tipicamente è lungo 1500 byte, in totale perchè IV si ripeta devono passare circa 25G di dati, che su una rete con 30Mbit/s di banda si ottengono in circa due ore.

IV corto

- come può l'attaccante sfruttare una debolezza del genere? esistono vari metodi:
  - esistono pacchetti di lunghezza fissa e contenuto prevedibile (es DHCP request). Se l'attaccante vede passare un pacchetto di quella lunghezza conosce il contenuto, può ricavare il keystream.
  - una volta ricavato un keystream può forgiare dei ping verso le macchine. Nella risposta ai ping devono essere contenuti i dati inviati nella richiesta, quindi la risposta è cifrata ma il contenuto prevedibile, quindi si ricavano altri keystream.
  - l'attaccante in questo modo si costruisce un intero dizionario di tutti i keystream e non ha più bisogno di conoscere la chiave segreta.
  - se non passano pacchetti DHCP l'attaccante può utilizzare l'attacco dell'oracolo

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

IV corto

- come può l'attaccante sfruttare una debolezza del genere? esistono vari metodi:
  - esistono pacchetti di lunghezza fissa e contenuto prevedibile (es DHCP request). Se l'attaccante vede passare un pacchetto di quella lunghezza conosce il contenuto, può ricavare il keystream.
  - una volta ricavato un keystream può forgiare dei ping verso le macchine. Nella risposta ai ping devono essere contenuti i dati inviati nella richiesta, quindi la risposta è cifrata ma il contenuto prevedibile, quindi si ricavano altri keystream.
  - l'attaccante in questo modo si costruisce un intero dizionario di tutti i keystream e non ha più bisogno di conoscere la chiave segreta.
  - se non passano pacchetti DHCP l'attaccante può utilizzare l'attacco dell'oracolo

IV corto

- come può l'attaccante sfruttare una debolezza del genere? esistono vari metodi:
  - esistono pacchetti di lunghezza fissa e contenuto prevedibile (es DHCP request). Se l'attaccante vede passare un pacchetto di quella lunghezza conosce il contenuto, può ricavare il keystream.
  - una volta ricavato un keystream può forgiare dei ping verso le macchine. Nella risposta ai ping devono essere contenuti i dati inviati nella richiesta, quindi la risposta è cifrata ma il contenuto prevedibile, quindi si ricavano altri keystream.
  - l'attaccante in questo modo si costruisce un intero dizionario di tutti i keystream e non ha più bisogno di conoscere la chiave segreta.
  - se non passano pacchetti DHCP l'attaccante può utilizzare l'attacco dell'oracolo

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

IV corto

- come può l'attaccante sfruttare una debolezza del genere? esistono vari metodi:
  - esistono pacchetti di lunghezza fissa e contenuto prevedibile (es DHCP request). Se l'attaccante vede passare un pacchetto di quella lunghezza conosce il contenuto, può ricavare il keystream.
  - una volta ricavato un keystream può forgiare dei ping verso le macchine. Nella risposta ai ping devono essere contenuti i dati inviati nella richiesta, quindi la risposta è cifrata ma il contenuto prevedibile, quindi si ricavano altri keystream.
  - l'attaccante in questo modo si costruisce un intero dizionario di tutti i keystream e non ha più bisogno di conoscere la chiave segreta.
  - se non passano pacchetti DHCP l'attaccante può utilizzare l'attacco dell'oracolo

IV corto

- come può l'attaccante sfruttare una debolezza del genere? esistono vari metodi:
  - esistono pacchetti di lunghezza fissa e contenuto prevedibile (es DHCP request). Se l'attaccante vede passare un pacchetto di quella lunghezza conosce il contenuto, può ricavare il keystream.
  - una volta ricavato un keystream può forgiare dei ping verso le macchine. Nella risposta ai ping devono essere contenuti i dati inviati nella richiesta, quindi la risposta è cifrata ma il contenuto prevedibile, quindi si ricavano altri keystream.
  - l'attaccante in questo modo si costruisce un intero dizionario di tutti i keystream e non ha più bisogno di conoscere la chiave segreta.
  - se non passano pacchetti DHCP l'attaccante può utilizzare l'attacco dell'oracolo

Problemi di checksum

- un keystream è lungo normalmente 1500 bytes ma con l'attacco dell'oracolo si ricavano solo 128 bytes, l'attaccante può estendere il keystream in qualche modo? ...
- ... ovviamente si, WEP viene incontro all'attaccante anche in questo caso :-)
  - si conoscono 128 byte di keystream, si invia un messaggio di ping di 129 bytes, l'ultimo si cifra estendendo il keystream con il byte 0x00. In fondo si mette il checksum fatto con CRC.
  - quando viene ricevuto il pacchetto a destinazione si verifica il checksum, se si riceve una risposta, evidentemente 0x00 era l'estensione corretta
  - se invece non si riceve risposta il checkusm è fallito, il pacchetto viene scartato, evidente 0x00 non era l'estensione giusta. Si riprova con 0x01. . . . Mediamente in 128 tentativi si trova un byte di estensione.
  - per estendere tutto un keystream bastano circa 24 ore

Problemi di checksum

- un keystream è lungo normalmente 1500 bytes ma con l'attacco dell'oracolo si ricavano solo 128 bytes, l'attaccante può estendere il keystream in qualche modo? ...
- ... ovviamente si, WEP viene incontro all'attaccante anche in questo caso :-)
  - si conoscono 128 byte di keystream, si invia un messaggio di ping di 129 bytes, l'ultimo si cifra estendendo il keystream con il byte 0x00. In fondo si mette il checksum fatto con CRC.
  - quando viene ricevuto il pacchetto a destinazione si verifica il checksum, se si riceve una risposta, evidentemente 0x00 era l'estensione corretta
  - se invece non si riceve risposta il checkusm è fallito, il pacchetto viene scartato, evidente 0x00 non era l'estensione giusta. Si riprova con 0x01. . . . Mediamente in 128 tentativi si trova un byte di estensione.
  - per estendere tutto un keystream bastano circa 24 ore

Problemi di checksum

- un keystream è lungo normalmente 1500 bytes ma con l'attacco dell'oracolo si ricavano solo 128 bytes, l'attaccante può estendere il keystream in qualche modo? ...
- ... ovviamente si, WEP viene incontro all'attaccante anche in questo caso :-)
  - si conoscono 128 byte di keystream, si invia un messaggio di ping di 129 bytes, l'ultimo si cifra estendendo il keystream con il byte 0x00. In fondo si mette il checksum fatto con CRC.
  - quando viene ricevuto il pacchetto a destinazione si verifica il checksum, se si riceve una risposta, evidentemente 0x00 era l'estensione corretta
  - se invece non si riceve risposta il checkusm è fallito, il pacchetto viene scartato, evidente 0x00 non era l'estensione giusta. Si riprova con 0x01. . . . Mediamente in 128 tentativi si trova un byte di estensione.
  - per estendere tutto un keystream bastano circa 24 ore

Problemi di checksum

- un keystream è lungo normalmente 1500 bytes ma con l'attacco dell'oracolo si ricavano solo 128 bytes, l'attaccante può estendere il keystream in qualche modo? ...
- ... ovviamente si, WEP viene incontro all'attaccante anche in questo caso :-)
  - si conoscono 128 byte di keystream, si invia un messaggio di ping di 129 bytes, l'ultimo si cifra estendendo il keystream con il byte 0x00. In fondo si mette il checksum fatto con CRC.
  - quando viene ricevuto il pacchetto a destinazione si verifica il checksum, se si riceve una risposta, evidentemente 0x00 era l'estensione corretta
  - se invece non si riceve risposta il checkusm è fallito, il pacchetto viene scartato, evidente 0x00 non era l'estensione giusta. Si riprova con 0x01. . . . Mediamente in 128 tentativi si trova un byte di estensione.
  - per estendere tutto un keystream bastano circa 24 ore

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Problemi di checksum

- un keystream è lungo normalmente 1500 bytes ma con l'attacco dell'oracolo si ricavano solo 128 bytes, l'attaccante può estendere il keystream in qualche modo? ...
- ... ovviamente si, WEP viene incontro all'attaccante anche in questo caso :-)
  - si conoscono 128 byte di keystream, si invia un messaggio di ping di 129 bytes, l'ultimo si cifra estendendo il keystream con il byte 0x00. In fondo si mette il checksum fatto con CRC.
  - quando viene ricevuto il pacchetto a destinazione si verifica il checksum, se si riceve una risposta, evidentemente 0x00 era l'estensione corretta
  - se invece non si riceve risposta il checkusm è fallito, il pacchetto viene scartato, evidente 0x00 non era l'estensione giusta. Si riprova con 0x01. . . . Mediamente in 128 tentativi si trova un byte di estensione.
  - per estendere tutto un keystream bastano circa 24 ore

Problemi di checksum

- un keystream è lungo normalmente 1500 bytes ma con l'attacco dell'oracolo si ricavano solo 128 bytes, l'attaccante può estendere il keystream in qualche modo? ...
- ... ovviamente si, WEP viene incontro all'attaccante anche in questo caso :-)
  - si conoscono 128 byte di keystream, si invia un messaggio di ping di 129 bytes, l'ultimo si cifra estendendo il keystream con il byte 0x00. In fondo si mette il checksum fatto con CRC.
  - quando viene ricevuto il pacchetto a destinazione si verifica il checksum, se si riceve una risposta, evidentemente 0x00 era l'estensione corretta
  - se invece non si riceve risposta il checkusm è fallito, il pacchetto viene scartato, evidente 0x00 non era l'estensione giusta. Si riprova con 0x01. . . . Mediamente in 128 tentativi si trova un byte di estensione.
  - per estendere tutto un keystream bastano circa 24 ore

Due calcoli

- Per avere accesso non autorizzato ad una rete 802.11 bisogna effettuare le seguenti operazioni:
  - attacco dell'oracolo $\leftarrow$ pochi secondi
  - estensione del keystream $\leftarrow$ 24 ore
  - generazione del dizionario $\leftarrow$ 3/4 ore
  - totale $\simeq$ 28 ore.
- se non si vuole rendere l'attacco troppo evidente bisogna diminuire il traffico generato e raddoppiare o triplicare il tempo occorrente
- ma se un'attaccante ha molta fretta, esistono metodi piu' rapidi?
- ovviamente, si.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Due calcoli

- Per avere accesso non autorizzato ad una rete 802.11 bisogna effettuare le seguenti operazioni:
  - attacco dell'oracolo $\leftarrow$ pochi secondi
  - estensione del keystream $\leftarrow$ 24 ore
  - generazione del dizionario $\leftarrow$ 3/4 ore
  - totale $\simeq$ 28 ore.
- se non si vuole rendere l'attacco troppo evidente bisogna diminuire il traffico generato e raddoppiare o triplicare il tempo occorrente
- ma se un'attaccante ha molta fretta, esistono metodi piu' rapidi?
- ovviamente, si.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Due calcoli

- Per avere accesso non autorizzato ad una rete 802.11 bisogna effettuare le seguenti operazioni:
  - attacco dell'oracolo $\leftarrow$ pochi secondi
  - estensione del keystream $\leftarrow$ 24 ore
  - generazione del dizionario $\leftarrow$ 3/4 ore
  - totale $\simeq$ 28 ore.
- se non si vuole rendere l'attacco troppo evidente bisogna diminuire il traffico generato e raddoppiare o triplicare il tempo occorrente
- ma se un'attaccante ha molta fretta, esistono metodi piu' rapidi?
- ovviamente, si.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Due calcoli

- Per avere accesso non autorizzato ad una rete 802.11 bisogna effettuare le seguenti operazioni:
  - attacco dell'oracolo $\leftarrow$ pochi secondi
  - estensione del keystream $\leftarrow$ 24 ore
  - generazione del dizionario $\leftarrow$ 3/4 ore
  - totale $\simeq$ 28 ore.
- se non si vuole rendere l'attacco troppo evidente bisogna diminuire il traffico generato e raddoppiare o triplicare il tempo occorrente
- ma se un'attaccante ha molta fretta, esistono metodi piu' rapidi?
- ovviamente, si.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Due calcoli

- Per avere accesso non autorizzato ad una rete 802.11 bisogna effettuare le seguenti operazioni:
  - attacco dell'oracolo $\leftarrow$ pochi secondi
  - estensione del keystream $\leftarrow$ 24 ore
  - generazione del dizionario $\leftarrow$ 3/4 ore
  - totale $\simeq$ 28 ore.
- se non si vuole rendere l'attacco troppo evidente bisogna diminuire il traffico generato e raddoppiare o triplicare il tempo occorrente
- ma se un'attaccante ha molta fretta, esistono metodi piu' rapidi?
- ovviamente, si.

Due calcoli

- Per avere accesso non autorizzato ad una rete 802.11 bisogna effettuare le seguenti operazioni:
  - attacco dell'oracolo $\leftarrow$ pochi secondi
  - estensione del keystream $\leftarrow$ 24 ore
  - generazione del dizionario $\leftarrow$ 3/4 ore
  - totale $\simeq$ 28 ore.
- se non si vuole rendere l'attacco troppo evidente bisogna diminuire il traffico generato e raddoppiare o triplicare il tempo occorrente
- ma se un'attaccante ha molta fretta, esistono metodi piu' rapidi?
- ovviamente, si.

Due calcoli

- Per avere accesso non autorizzato ad una rete 802.11 bisogna effettuare le seguenti operazioni:
  - attacco dell'oracolo $\leftarrow$ pochi secondi
  - estensione del keystream $\leftarrow$ 24 ore
  - generazione del dizionario $\leftarrow$ 3/4 ore
  - totale $\simeq$ 28 ore.
- se non si vuole rendere l'attacco troppo evidente bisogna diminuire il traffico generato e raddoppiare o triplicare il tempo occorrente
- ma se un'attaccante ha molta fretta, esistono metodi piu' rapidi?
- ovviamente, si.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Vulnerabilità di RC4

- Nel 2001 i signori Fluhrer, Mantin e Shamir trovano una vulnerabilità nel modo in cui RC4 genera i keystream.
  - quando si utilizzano determinati IV per generare il keystream esiste una correlazione tra i primi due byte del keystream e la chiave segreta utilizzata
  - raccogliendo almeno 60 pacchetti cifrati a partire da IV *interessanti* si può ricavare una chiave segreta!
  - per ottenere 60 IV interessanti ci vogliono mediamente 4.000.000 di pacchetti cifrati
  - a seconda del traffico generato dalla rete in poche ore si rompe una chiave WEP e si ottiene una chiave segreta a 40 bit!
  - la complessità aumenta linearmente con la lunghezza della chiave, quindi aumentare la lunghezza della chiave non impedisce l'attacco

nell'agosto 2004 l'hacker KoreK invia su un forum un tool basato su una sua ricerca statistica. attualmente per rompere una chiave WEP a 40 bit basta raccogliere circa 200.000 pacchetti cifrati e attendere un tempo di elaborazione di pochi secondi.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Vulnerabilità di RC4

- Nel 2001 i signori Fluhrer, Mantin e Shamir trovano una vulnerabilità nel modo in cui RC4 genera i keystream.
  - quando si utilizzano determinati IV per generare il keystream esiste una correlazione tra i primi due byte del keystream e la chiave segreta utilizzata
  - raccogliendo almeno 60 pacchetti cifrati a partire da IV *interessanti* si può ricavare una chiave segreta!
  - per ottenere 60 IV interessanti ci vogliono mediamente 4.000.000 di pacchetti cifrati
  - a seconda del traffico generato dalla rete in poche ore si rompe una chiave WEP e si ottiene una chiave segreta a 40 bit!
  - la complessità aumenta linearmente con la lunghezza della chiave, quindi aumentare la lunghezza della chiave non impedisce l'attacco

nell'agosto 2004 l'hacker KoreK invia su un forum un tool basato su una sua ricerca statistica. attualmente per rompere una chiave WEP a 40 bit basta raccogliere circa 200.000 pacchetti cifrati e attendere un tempo di elaborazione di pochi secondi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Vulnerabilità di RC4

- Nel 2001 i signori Fluhrer, Mantin e Shamir trovano una vulnerabilità nel modo in cui RC4 genera i keystream.
  - quando si utilizzano determinati IV per generare il keystream esiste una correlazione tra i primi due byte del keystream e la chiave segreta utilizzata
  - raccogliendo almeno 60 pacchetti cifrati a partire da IV *interessanti* si può ricavare una chiave segreta!
  - per ottenere 60 IV interessanti ci vogliono mediamente 4.000.000 di pacchetti cifrati
  - a seconda del traffico generato dalla rete in poche ore si rompe una chiave WEP e si ottiene una chiave segreta a 40 bit!
  - la complessità aumenta linearmente con la lunghezza della chiave, quindi aumentare la lunghezza della chiave non impedisce l'attacco

nell'agosto 2004 l'hacker KoreK invia su un forum un tool basato su una sua ricerca statistica. attualmente per rompere una chiave WEP a 40 bit basta raccogliere circa 200.000 pacchetti cifrati e attendere un tempo di elaborazione di pochi secondi.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Vulnerabilità di RC4

- Nel 2001 i signori Fluhrer, Mantin e Shamir trovano una vulnerabilità nel modo in cui RC4 genera i keystream.
  - quando si utilizzano determinati IV per generare il keystream esiste una correlazione tra i primi due byte del keystream e la chiave segreta utilizzata
  - raccogliendo almeno 60 pacchetti cifrati a partire da IV *interessanti* si può ricavare una chiave segreta!
  - per ottenere 60 IV interessanti ci vogliono mediamente 4.000.000 di pacchetti cifrati
  - a seconda del traffico generato dalla rete in poche ore si rompe una chiave WEP e si ottiene una chiave segreta a 40 bit!
  - la complessità aumenta linearmente con la lunghezza della chiave, quindi aumentare la lunghezza della chiave non impedisce l'attacco

nell'agosto 2004 l'hacker KoreK invia su un forum un tool basato su una sua ricerca statistica. attualmente per rompere una chiave WEP a 40 bit basta raccogliere circa 200.000 pacchetti cifrati e attendere un tempo di elaborazione di pochi secondi.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Vulnerabilità di RC4

- Nel 2001 i signori Fluhrer, Mantin e Shamir trovano una vulnerabilità nel modo in cui RC4 genera i keystream.
  - quando si utilizzano determinati IV per generare il keystream esiste una correlazione tra i primi due byte del keystream e la chiave segreta utilizzata
  - raccogliendo almeno 60 pacchetti cifrati a partire da IV *interessanti* si può ricavare una chiave segreta!
  - per ottenere 60 IV interessanti ci vogliono mediamente 4.000.000 di pacchetti cifrati
  - a seconda del traffico generato dalla rete in poche ore si rompe una chiave WEP e si ottiene una chiave segreta a 40 bit!
  - la complessità aumenta linearmente con la lunghezza della chiave, quindi aumentare la lunghezza della chiave non impedisce l'attacco

nell'agosto 2004 l'hacker KoreK invia su un forum un tool basato su una sua ricerca statistica. attualmente per rompere una chiave WEP a 40 bit basta raccogliere circa 200.000 pacchetti cifrati e attendere un tempo di elaborazione di pochi secondi.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Vulnerabilità di RC4

- Nel 2001 i signori Fluhrer, Mantin e Shamir trovano una vulnerabilità nel modo in cui RC4 genera i keystream.
  - quando si utilizzano determinati IV per generare il keystream esiste una correlazione tra i primi due byte del keystream e la chiave segreta utilizzata
  - raccogliendo almeno 60 pacchetti cifrati a partire da IV *interessanti* si può ricavare una chiave segreta!
  - per ottenere 60 IV interessanti ci vogliono mediamente 4.000.000 di pacchetti cifrati
  - a seconda del traffico generato dalla rete in poche ore si rompe una chiave WEP e si ottiene una chiave segreta a 40 bit!
  - la complessità aumenta linearmente con la lunghezza della chiave, quindi aumentare la lunghezza della chiave non impedisce l'attacco

nell'agosto 2004 l'hacker KoreK invia su un forum un tool basato su una sua ricerca statistica. attualmente per rompere una chiave WEP a 40 bit basta raccogliere circa 200.000 pacchetti cifrati e attendere un tempo di elaborazione di pochi secondi.

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Vulnerabilità di CRC-32

- per finire, l'algoritmo che viene utilizzato per l'identificazione di errori o manomissioni, CRC-32 è un algorimo lineare
- questo permette ad un attaccante che non conosce la chiave di cambiare il contenuto di un pacchetto senza che il destinatario possa accorgersene

→ si possono redirigere i pacchetti cifrati verso l'esterno della rete cambiando l'indirizzo IP destinazione. L'AP li decifrerà e instraderà verso l'esterno

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Vulnerabilità di CRC-32

- per finire, l'algoritmo che viene utilizzato per l'identificazione di errori o manomissioni, CRC-32 è un algorimo lineare
- questo permette ad un attaccante che non conosce la chiave di cambiare il contenuto di un pacchetto senza che il destinatario possa accorgersene

→ si possono redirigere i pacchetti cifrati verso l'esterno della rete cambiando l'indirizzo IP destinazione. L'AP li decifrerà e instraderà verso l'esterno

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Vulnerabilità di CRC-32

- per finire, l'algoritmo che viene utilizzato per l'identificazione di errori o manomissioni, CRC-32 è un algorimo lineare
- questo permette ad un attaccante che non conosce la chiave di cambiare il contenuto di un pacchetto senza che il destinatario possa accorgersene

→ si possono redirigere i pacchetti cifrati verso l'esterno della rete cambiando l'indirizzo IP destinazione. L'AP li decifrerà e instraderà verso l'esterno

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Conclusioni

- WEP non garantisce la disponibilità del servizio (deauth attack)
- WEP non garantisce l'integrità dei dati (CRC lineare)
- WEP non garantisce l'autenticazione, la segretezza, la non ripudiabilità dei dati (chiavi craccabili)
- WEP non garantisce il controllo degli accessi (autenticazione cosí ridicola da essere stata abbandonata da tutti i produttori)

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Conclusioni

- WEP non garantisce la disponibilità del servizio (deauth attack)
- WEP non garantisce l'integrità dei dati (CRC lineare)
- WEP non garantisce l'autenticazione, la segretezza, la non ripudiabilità dei dati (chiavi craccabili)
- WEP non garantisce il controllo degli accessi (autenticazione cosí ridicola da essere stata abbandonata da tutti i produttori)

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Conclusioni

- WEP non garantisce la disponibilità del servizio (deauth attack)
- WEP non garantisce l'integrità dei dati (CRC lineare)
- WEP non garantisce l'autenticazione, la segretezza, la non ripudiabilità dei dati (chiavi craccabili)
- WEP non garantisce il controllo degli accessi (autenticazione cosí ridicola da essere stata abbandonata da tutti i produttori)

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Conclusioni

- WEP non garantisce la disponibilità del servizio (deauth attack)
- WEP non garantisce l'integrità dei dati (CRC lineare)
- WEP non garantisce l'autenticazione, la segretezza, la non ripudiabilità dei dati (chiavi craccabili)
- WEP non garantisce il controllo degli accessi (autenticazione cosí ridicola da essere stata abbandonata da tutti i produttori)

standard 802.11i

802.11i viene definito per porre rimedio alle insicurezze di 802.11.

- si introduce un nuovo elemento nella rete, l'authentication server, AS
- quando un host entra nella rete si autentica non più con l'AP ma con l'AS, che contiene un database di credenziali di macchine abilitate a entrare
- l'AP in questa fase fa solo da proxy verso l'AS, veicolando i pacchetti di autenticazione
- successivamente l'AP riceve dall'AS le chiavi segrete che sono state negoziate tra il client e l'AS, a quel punto può comunicare con il client

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

standard 802.11i

802.11i viene definito per porre rimedio alle insicurezze di 802.11.

- si introduce un nuovo elemento nella rete, l'authentication server, AS
- quando un host entra nella rete si autentica non più con l'AP ma con l'AS, che contiene un database di credenziali di macchine abilitate a entrare
- l'AP in questa fase fa solo da proxy verso l'AS, veicolando i pacchetti di autenticazione
- successivamente l'AP riceve dall'AS le chiavi segrete che sono state negoziate tra il client e l'AS, a quel punto può comunicare con il client

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

standard 802.11i

802.11i viene definito per porre rimedio alle insicurezze di 802.11.

- si introduce un nuovo elemento nella rete, l'authentication server, AS
- quando un host entra nella rete si autentica non più con l'AP ma con l'AS, che contiene un database di credenziali di macchine abilitate a entrare
- l'AP in questa fase fa solo da proxy verso l'AS, veicolando i pacchetti di autenticazione
- successivamente l'AP riceve dall'AS le chiavi segrete che sono state negoziate tra il client e l'AS, a quel punto può comunicare con il client

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

standard 802.11i

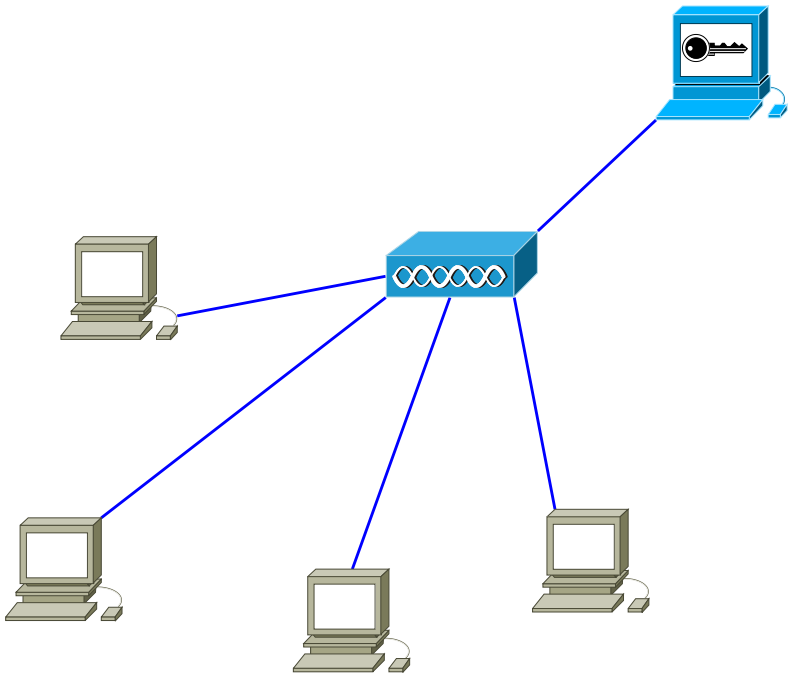
802.11i viene definito per porre rimedio alle insicurezze di 802.11.

- si introduce un nuovo elemento nella rete, l'authentication server, AS
- quando un host entra nella rete si autentica non più con l'AP ma con l'AS, che contiene un database di credenziali di macchine abilitate a entrare
- l'AP in questa fase fa solo da proxy verso l'AS, veicolando i pacchetti di autenticazione
- successivamente l'AP riceve dall'AS le chiavi segrete che sono state negoziate tra il client e l'AS, a quel punto può comunicare con il client

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Cambio di modello

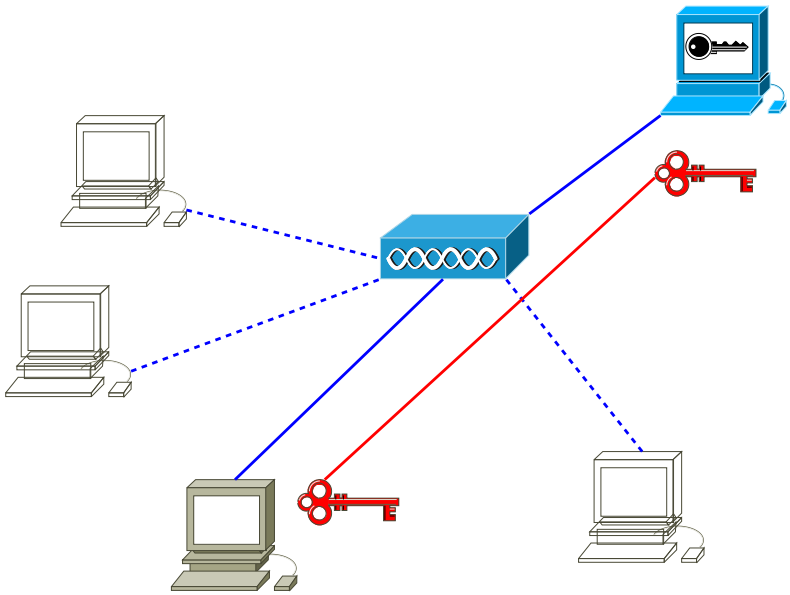


- il client scambia messaggi con l'AS attraverso l'AP
- il client genera una chiave PMK con AS
- PMK viene spostata su AP
- A partire da PMK l'AP e il client generano una nuova chiave di sessione PTK con cui comunicano

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Cambio di modello

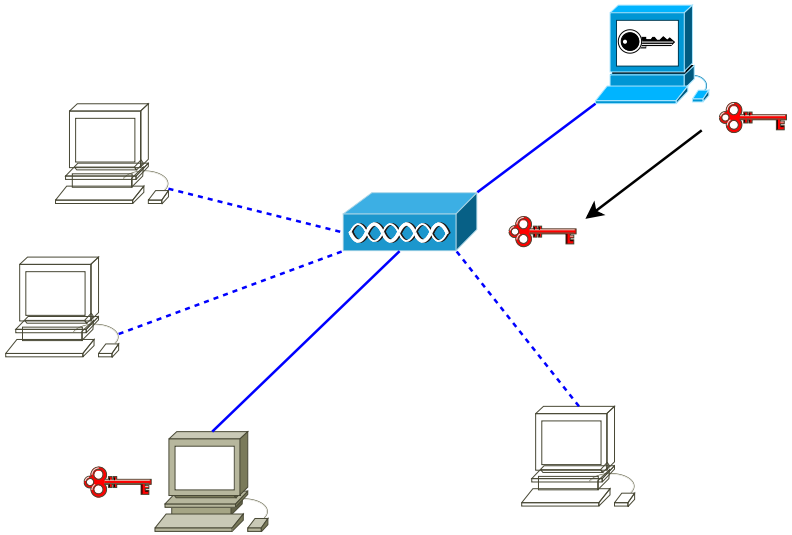


- il client scambia messaggi con l'AS attraverso l'AP
- il client genera una chiave PMK con AS
- PMK viene spostata su AP
- A partire da PMK l'AP e il client generano una nuova chiave di sessione PTK con cui comunicano

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Cambio di modello

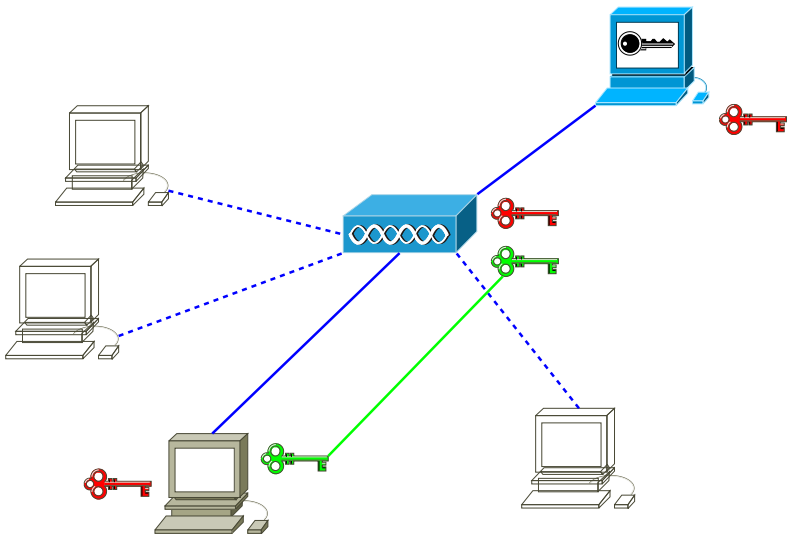


- il client scambia messaggi con l'AS attraverso l'AP
- il client genera una chiave PMK con AS
- PMK viene spostata su AP
- A partire da PMK l'AP e il client generano una nuova chiave di sessione PTK con cui comunicano

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Cambio di modello



- il client scambia messaggi con l'AS attraverso l'AP
- il client genera una chiave PMK con AS
- PMK viene spostata su AP
- A partire da PMK l'AP e il client generano una nuova chiave di sessione PTK con cui comunicano

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Cambio di algoritmi

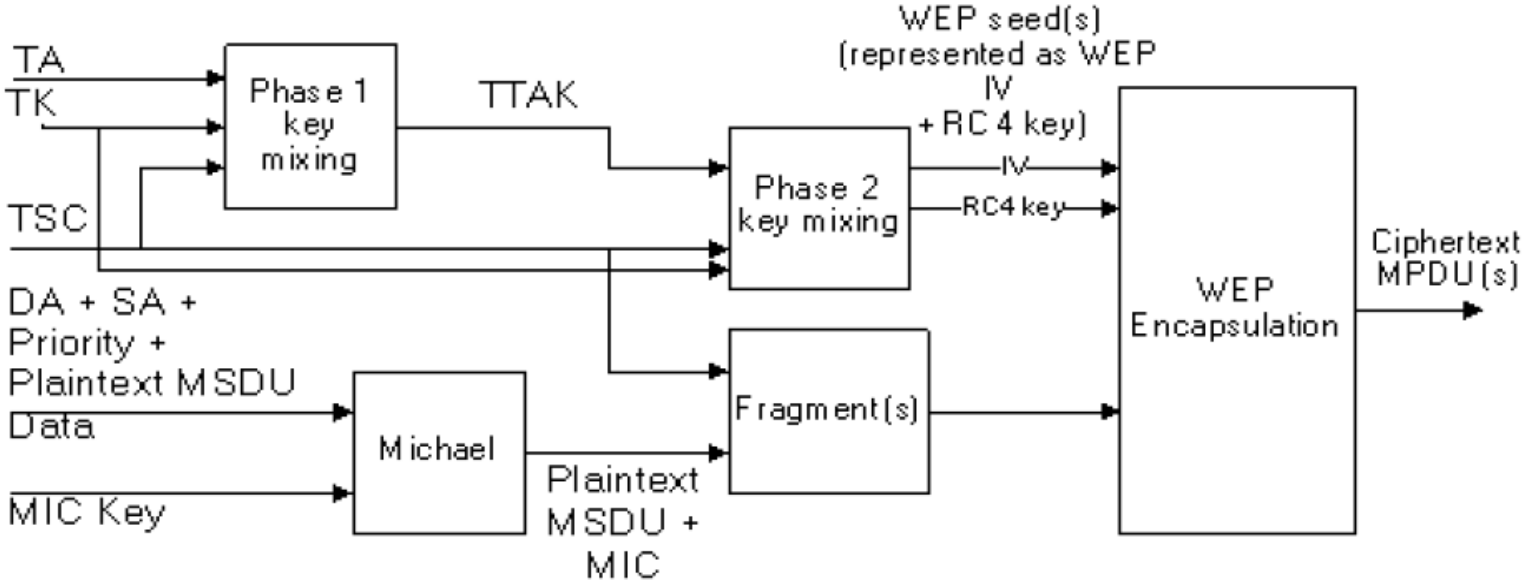
Si utilizzano due algoritmi al posto di WEP, il TKIP o il CCMP, entrambi eliminano le problematiche di sicurezza riguardanti IV corti, chiavi craccabili, CRC ecc. . . , introducono però maggiore complessità, quindi difficilmente sono stati portati su hardware esistente

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Cambio di algoritmi

Si utilizzano due algoritmi al posto di WEP, il TKIP o il CCMP, entrambi eliminano le problematiche di sicurezza riguardanti IV corti, chiavi craccabili, CRC ecc. . . , introducono però maggiore complessità, quindi difficilmente sono stati portati su hardware esistente



Miglioramenti

- L'autenticazione viene veicolata attraverso l'AP ma l'AP non ne prende parte:
  - l'AP è alleggerito di alcune funzioni
  - il tipo di autenticazione è un parametro, può essere modificata riconfigurando AS e client
  - si introduce un meccanismo di refresh delle chiavi (le PTK possono essere rinegoziate periodicamente)
  - la PTK è diversa per ogni client

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Miglioramenti

- L'autenticazione viene veicolata attraverso l'AP ma l'AP non ne prende parte:
  - l'AP è alleggerito di alcune funzioni
  - il tipo di autenticazione è un parametro, può essere modificata riconfigurando AS e client
  - si introduce un meccanismo di refresh delle chiavi (le PTK possono essere rinegoziate periodicamente)
  - la PTK è diversa per ogni client

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Miglioramenti

- L'autenticazione viene veicolata attraverso l'AP ma l'AP non ne prende parte:
  - l'AP è alleggerito di alcune funzioni
  - il tipo di autenticazione è un parametro, può essere modificata riconfigurando AS e client
  - si introduce un meccanismo di refresh delle chiavi (le PTK possono essere rinegoziate periodicamente)
  - la PTK è diversa per ogni client

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Miglioramenti

- L'autenticazione viene veicolata attraverso l'AP ma l'AP non ne prende parte:
  - l'AP è alleggerito di alcune funzioni
  - il tipo di autenticazione è un parametro, può essere modificata riconfigurando AS e client
  - si introduce un meccanismo di refresh delle chiavi (le PTK possono essere rinegoziate periodicamente)
  - la PTK è diversa per ogni client

Leonardo Maccari,
maccari@lenst.det.unifi.

Descrizione di 802.11
Funzionamento generale
Wireless Equivalent Privacy
Sicurezza di 802.11
Denial of service
Attacchi sull'autenticazione
Gestione delle chiavi
Debolezza degli algoritmi
Protocollo 802.11i
Introduzione

Miglioramenti

- L'autenticazione viene veicolata attraverso l'AP ma l'AP non ne prende parte:
  - l'AP è alleggerito di alcune funzioni
  - il tipo di autenticazione è un parametro, può essere modificata riconfigurando AS e client
  - si introduce un meccanismo di refresh delle chiavi (le PTK possono essere rinegoziate periodicamente)
  - la PTK è diversa per ogni client

bibliografia

- Unsafe at any key size: http://www.dis.org/wl/pdf/unsafe.pdf
- 802.11i overview: http://csrc.nist.gov/wireless/S10_802.11i%20Overview-jw1.pdf