Il protocollo 802.11i

Leonardo Maccari,
maccari@lart.det.unifi.it

Slides per il corso di Gestione delle reti di telecomunicazioni

17 marzo 2006

Principi di crittografia:
- Cifratura a chiave simmetrica
- Cifratura a chiave pubblica/privata
- Funzioni hash
- Certificati

Il protocollo 802.11i
- 802.1X e 802.11i
- Protocolli coinvolti
- Metodi EAP
- Protocolli di tunnel
- RADIUS vulnerability

WPA-PSK

La crittografia garantisce:

- Protezione dei documenti
  - integrità
  - confidenzialità
  - autenticazione
  - non ripudiabilità
- Verifica dell'identità dei corrispondenti

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Protezione dei documenti
  - integrità
  - confidenzialità
  - autenticazione
  - non ripudiabilità
- Verifica dell'identità dei corrispondenti

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Protezione dei documenti
  - integrità
  - confidenzialità
  - autenticazione
  - non ripudiabilità
- Verifica dell'identità dei corrispondenti

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Protezione dei documenti
  - integrità
  - confidenzialità
  - autenticazione
  - non ripudiabilità
- Verifica dell'identità dei corrispondenti
  - autenticazione
  - non ripudiabilità

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Protezione dei documenti
  - integrità
  - confidenzialità
  - autenticazione
  - non ripudiabilità
- Verifica dell'identità dei corrispondenti
  - certificazione
  - autorizzazione

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Protezione dei documenti
  - integrità
  - confidenzialità
  - autenticazione
  - non ripudiabilità
- Verifica dell'identità dei corrispondenti
  - certificazione
  - autorizzazione

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Protezione dei documenti
  - integrità
  - confidenzialità
  - autenticazione
  - non ripudiabilità
- Verifica dell'identità dei corrispondenti
  - certificazione
  - autorizzazione

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Protezione dei documenti
  - integrità
  - confidenzialità
  - autenticazione
  - non ripudiabilità
- Verifica dell'identità dei corrispondenti
  - certificazione
  - autorizzazione

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Elementi di un sistema crittografico:
  - cifrario (algoritmo)
  - chiave (informazione)
- Principio di Kerchoffs

- La conoscenza della chiave

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Elementi di un sistema crittografico:
  - cifrario (algoritmo)
  - chiave (informazione)
- Principio di Kerchoffs
  - Il nemico ha accesso ma non a tutto
  - Il segreto risiede nella chiave
- La conoscenza della chiave

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Elementi di un sistema crittografico:
  - cifrario (algoritmo)
  - chiave (informazione)
- Principio di Kerchoffs
  - il metodo si suppone noto a tutti
  - il segreto risiede nella chiave
- La conoscenza della chiave

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Elementi di un sistema crittografico:
  - cifrario (algoritmo)
  - chiave (informazione)
- Principio di Kerchoffs
  - il metodo si suppone noto a tutti
  - il segreto risiede nella chiave
- La conoscenza della chiave

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Elementi di un sistema crittografico:
  - cifrario (algoritmo)
  - chiave (informazione)
- Principio di Kerchoffs
  - il metodo si suppone noto a tutti
  - il segreto risiede nella chiave
- La conoscenza della chiave
  - consente di cifrare/decifrare il messaggio
  - rende crittograficamente forte un cifrario debole

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Elementi di un sistema crittografico:
  - cifrario (algoritmo)
  - chiave (informazione)
- Principio di Kerchoffs
  - il metodo si suppone noto a tutti
  - il segreto risiede nella chiave
- La conoscenza della chiave
  - consente di cifrare/decifrare documenti
  - può costituire prova certa di identità

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Elementi di un sistema crittografico:
  - cifrario (algoritmo)
  - chiave (informazione)
- Principio di Kerchoffs
  - il metodo si suppone noto a tutti
  - il segreto risiede nella chiave
- La conoscenza della chiave
  - consente di cifrare/decifrare documenti
  - può costituire prova certa di identità

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Elementi di un sistema crittografico:
  - cifrario (algoritmo)
  - chiave (informazione)
- Principio di Kerchoffs
  - il metodo si suppone noto a tutti
  - il segreto risiede nella chiave
- La conoscenza della chiave
  - consente di cifrare/decifrare documenti
  - può costituire prova certa di identità

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

La crittografia garantisce:

- Elementi di un sistema crittografico:
  - cifrario (algoritmo)
  - chiave (informazione)
- Principio di Kerchoffs
  - il metodo si suppone noto a tutti
  - il segreto risiede nella chiave
- La conoscenza della chiave
  - consente di cifrare/decifrare documenti
  - può costituire prova certa di identità

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Chiave simmetrica

- unica chiave
- la chiave va concordata tra mittente e destinatario prima dello scambio dei dati
- problema di trasmissione sicura della chiave

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Chiave simmetrica

- unica chiave
- la chiave va concordata tra mittente e destinatario prima dello scambio dei dati
- problema di trasmissione sicura della chiave

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

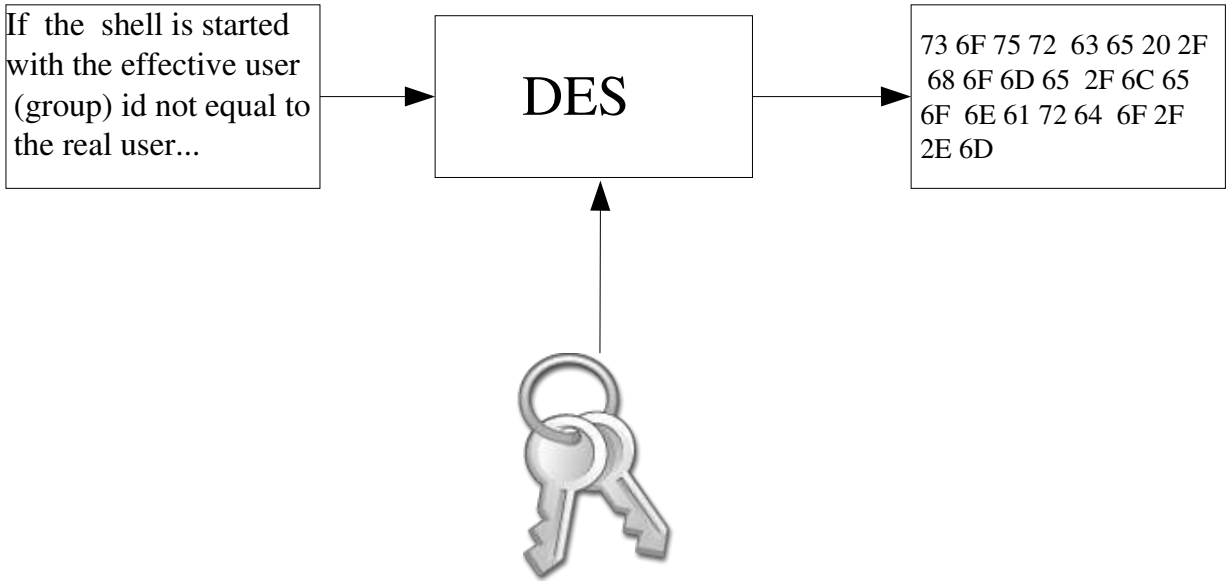
Chiave simmetrica

- unica chiave
- la chiave va concordata tra mittente e destinatario prima dello scambio dei dati
- problema di trasmissione sicura della chiave

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

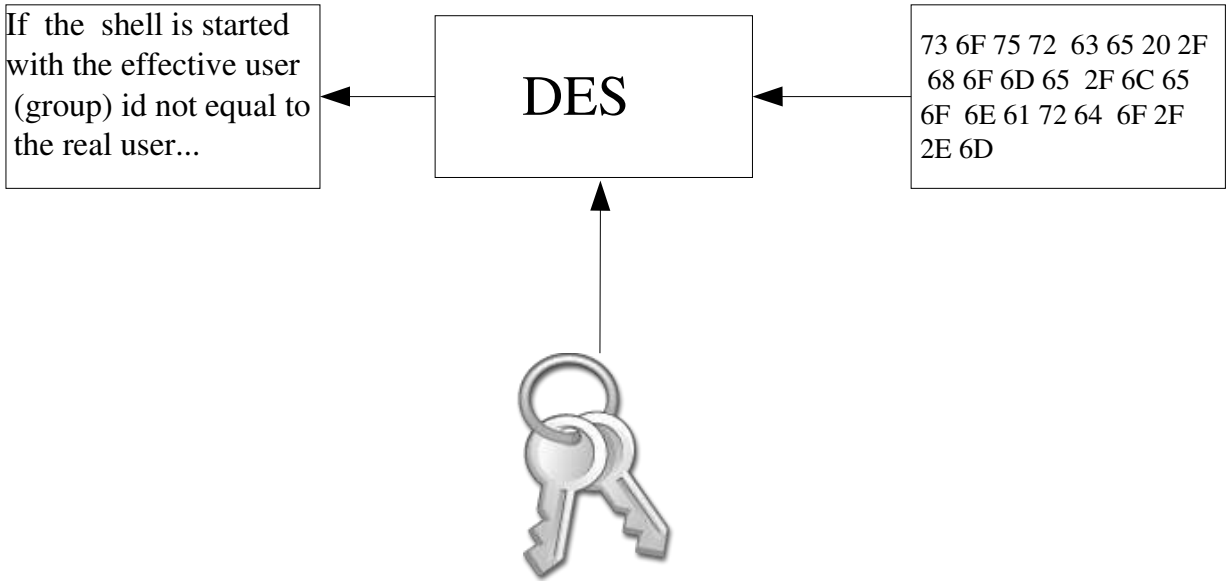
Cifratura



Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Decifratura



Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Cifratura a chiave pubblica/privata

- Ogni soggetto possiede una coppia di chiavi
  - Chiave publica
  - Chiave privata
- Ciò che viene cifrato con una chiave può essere decifrato solo con l'altra
- E' computazionalmente impossibile risalire ad una chiave privata tramite la chiave pubblica

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Cifratura a chiave pubblica/privata

- Ogni soggetto possiede una coppia di chiavi
  - Chiave publica
  - Chiave privata
- Ciò che viene cifrato con una chiave può essere decifrato solo con l'altra
- E' computazionalmente impossibile risalire ad una chiave privata tramite la chiave pubblica

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Cifratura a chiave pubblica/privata

- Ogni soggetto possiede una coppia di chiavi
  - Chiave publica
  - Chiave privata
- Ciò che viene cifrato con una chiave può essere decifrato solo con l'altra
- E' computazionalmente impossibile risalire ad una chiave privata tramite la chiave pubblica

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Cifratura a chiave pubblica/privata

- Ogni soggetto possiede una coppia di chiavi
  - Chiave publica
  - Chiave privata
- Ciò che viene cifrato con una chiave può essere decifrato solo con l'altra
- E' computazionalmente impossibile risalire ad una chiave privata tramite la chiave pubblica

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Cifratura a chiave pubblica/privata

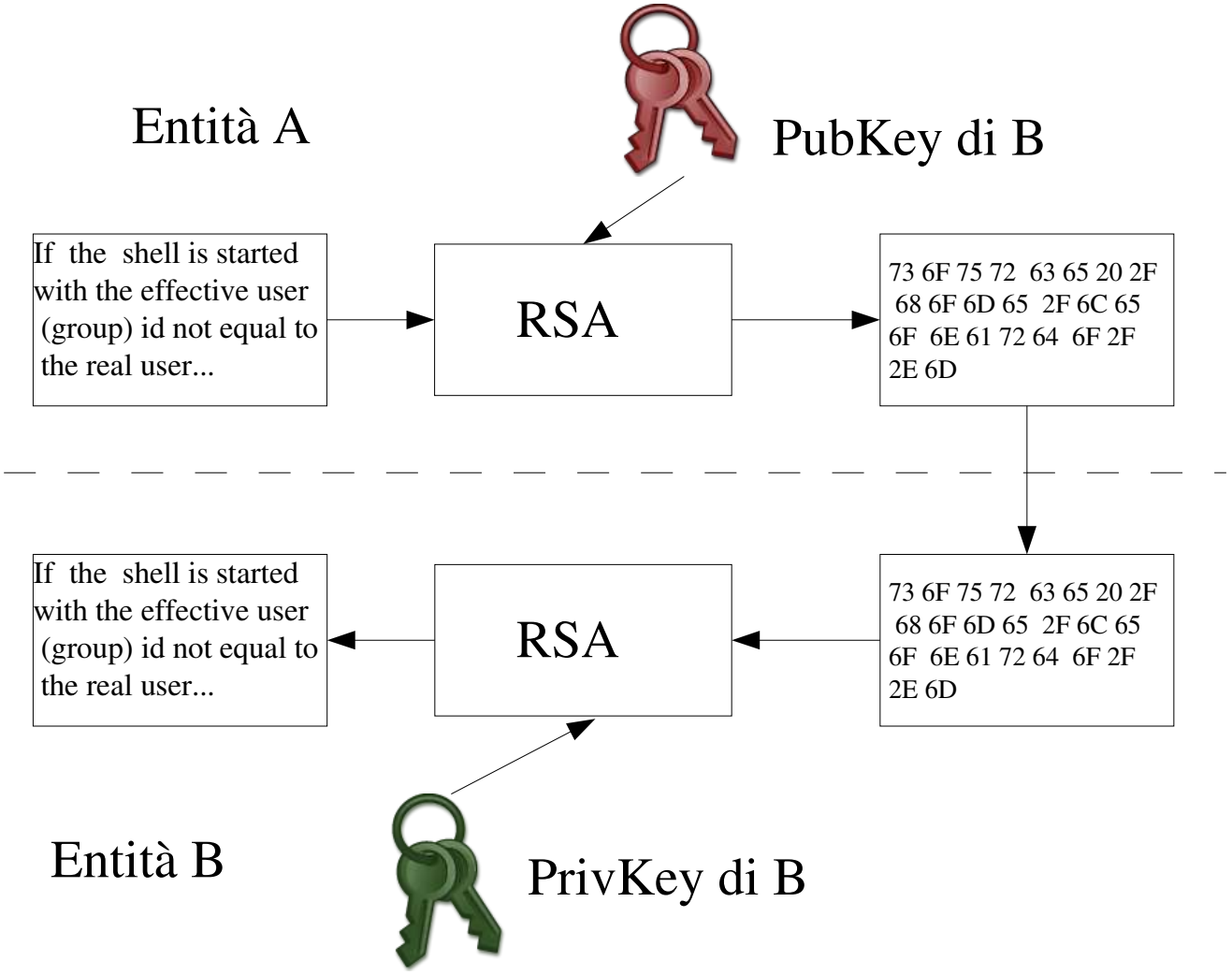
- Ogni soggetto possiede una coppia di chiavi
  - Chiave publica
  - Chiave privata
- Ciò che viene cifrato con una chiave può essere decifrato solo con l'altra
- E' computazionalmente impossibile risalire ad una chiave privata tramite la chiave pubblica

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Cifratura e Decifratura

Solo B, conoscendo la chiave PrivKey, può decifrare il documento, si ottiene: riservatezza



Principi di crittografia:
- Cifratura a chiave simmetrica
- Cifratura a chiave pubblica/privata
- Funzioni hash
- Certificati

Il protocollo 802.11i
- 802.1X e 802.11i
- Protocolli coinvolti
- Metodi EAP
- Protocolli di tunnel
- RADIUS vulnerability

WPA-PSK

Riassumendo

- Ogni utente ha due chiavi legate in modo inscindibile da una formula matematica
  - una chiave viene resa pubblica
  - l'altra è in possesso del solo utente
- le chiavi pubbliche sono disponibili in un elenco centralizzato consultabile liberamente dagli utenti
- le coppie di chiavi pubbliche/private sono generate a cura dell'utente

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Riassumendo

- Ogni utente ha due chiavi legate in modo inscindibile da una formula matematica
  - una chiave viene resa pubblica
  - l'altra è in possesso del solo utente
- le chiavi pubbliche sono disponibili in un elenco centralizzato consultabile liberamente dagli utenti
- le coppie di chiavi pubbliche/private sono generate a cura dell'utente

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Riassumendo

- Ogni utente ha due chiavi legate in modo inscindibile da una formula matematica
  - una chiave viene resa pubblica
  - l'altra è in possesso del solo utente
- le chiavi pubbliche sono disponibili in un elenco centralizzato consultabile liberamente dagli utenti
- le coppie di chiavi pubbliche/private sono generate a cura dell'utente

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Riassumendo

- Ogni utente ha due chiavi legate in modo inscindibile da una formula matematica
  - una chiave viene resa pubblica
  - l'altra è in possesso del solo utente
- le chiavi pubbliche sono disponibili in un elenco centralizzato consultabile liberamente dagli utenti
- le coppie di chiavi pubbliche/private sono generate a cura dell'utente

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Riassumendo

- Ogni utente ha due chiavi legate in modo inscindibile da una formula matematica
  - una chiave viene resa pubblica
  - l'altra è in possesso del solo utente
- le chiavi pubbliche sono disponibili in un elenco centralizzato consultabile liberamente dagli utenti
- le coppie di chiavi pubbliche/private sono generate a cura dell'utente

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

- Non è necessario concordare preventivamente una chiave di cifratura comune per scambiarsi un documento riservato
- La chiave privata di un utente è sempre segreta
- Attraverso la firma digitale si autenticano i propri messaggi in modo certo ed inequivocabile

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

- Non è necessario concordare preventivamente una chiave di cifratura comune per scambiarsi un documento riservato
- La chiave privata di un utente è sempre segreta
- Attraverso la firma digitale si autenticano i propri messaggi in modo certo ed inequivocabile

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

- Non è necessario concordare preventivamente una chiave di cifratura comune per scambiarsi un documento riservato
- La chiave privata di un utente è sempre segreta
- Attraverso la firma digitale si autenticano i propri messaggi in modo certo ed inequivocabile

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

- Funzione di hash
  - genera una impronta (digest) dei dati
  - non è reversibile (dal digest non si può ricavare il dato)

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

- Funzione di hash
  - genera una impronta (digest) dei dati
  - non è reversibile (dal digest non si può ricavare il dato)

Leonardo Maccari,
maccari@lart.det.unifi.it

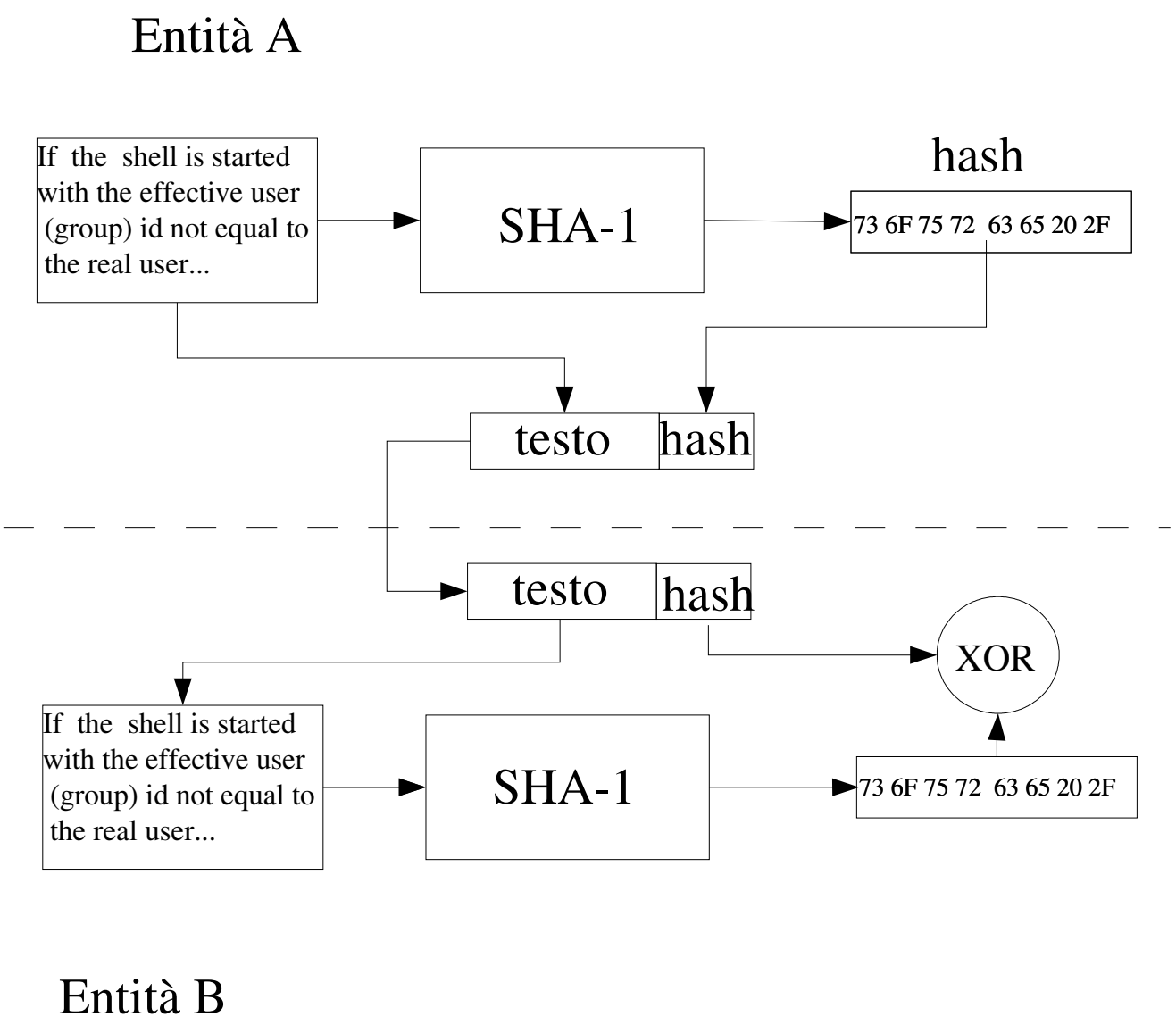
Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

- Funzione di hash
  - genera una impronta (digest) dei dati
  - non è reversibile (dal digest non si può ricavare il dato)

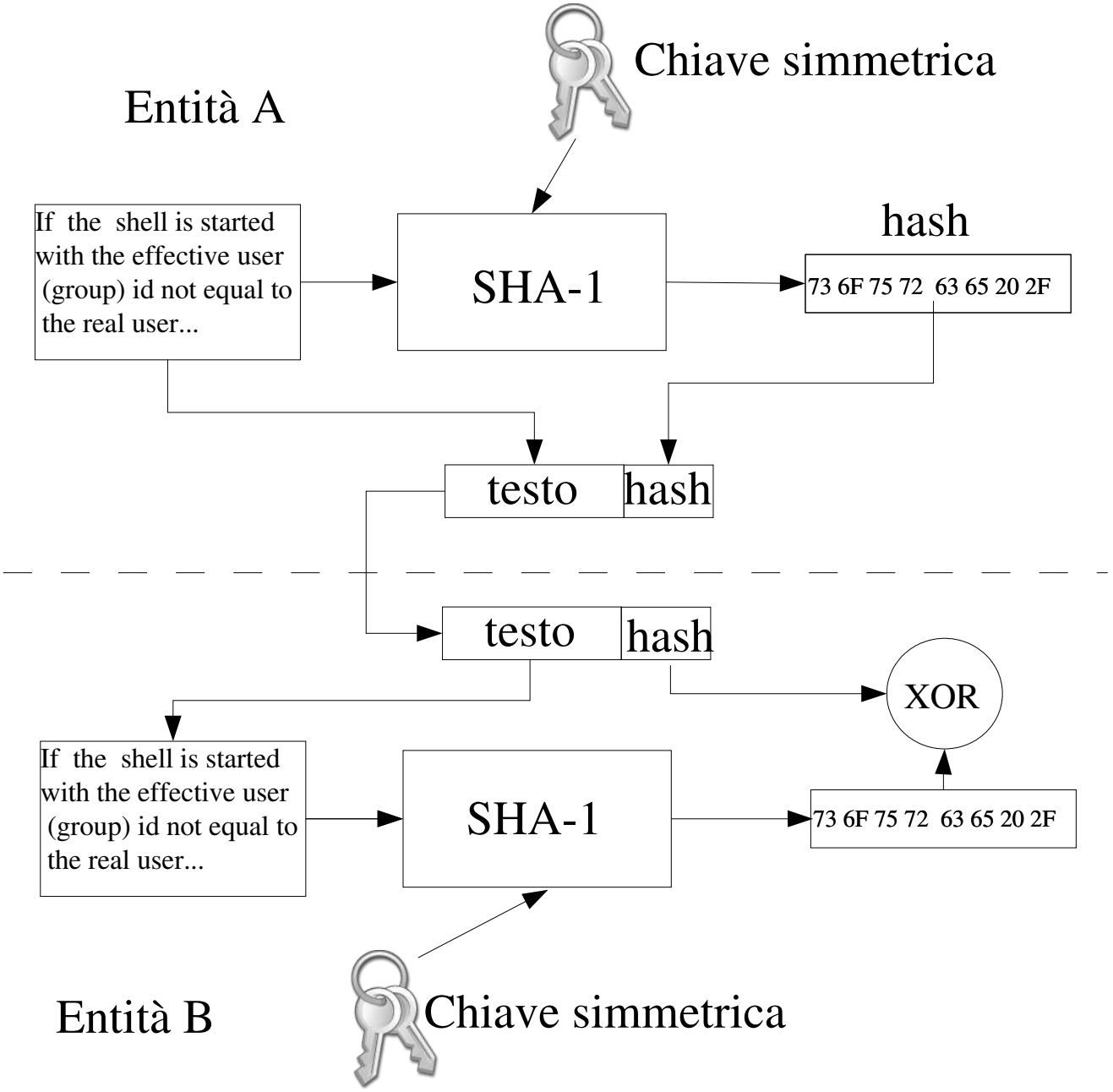
Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Hashing


Entità A
If the shell is started with the effective user (group) id not equal to the real user...
SHA-1
hash
73 6F 75 72 63 65 20 2F
testo
hash
testo
hash
XOR
If the shell is started with the effective user (group) id not equal to the real user...
SHA-1
73 6F 75 72 63 65 20 2F
Entità B

HMAC



Principi di crittografia:
- Cifratura a chiave simmetrica
- Cifratura a chiave pubblica/privata
- Funzioni hash
- Certificati

Il protocollo 802.11i
- 802.1X e 802.11i
- Protocolli coinvolti
- Metodi EAP
- Protocolli di tunnel
- RADIUS vulnerability

WPA-PSK

Firma digitale

- Le chiavi pubblica e privata sono invertibili
- Si può cifrare con la privata e decifrare con la pubblica
- Chi decifra è anche sicuro dell'identità del mittente

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Firma digitale

- Le chiavi pubblica e privata sono invertibili
- Si può cifrare con la privata e decifrare con la pubblica
- Chi decifra è anche sicuro dell'identità del mittente

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

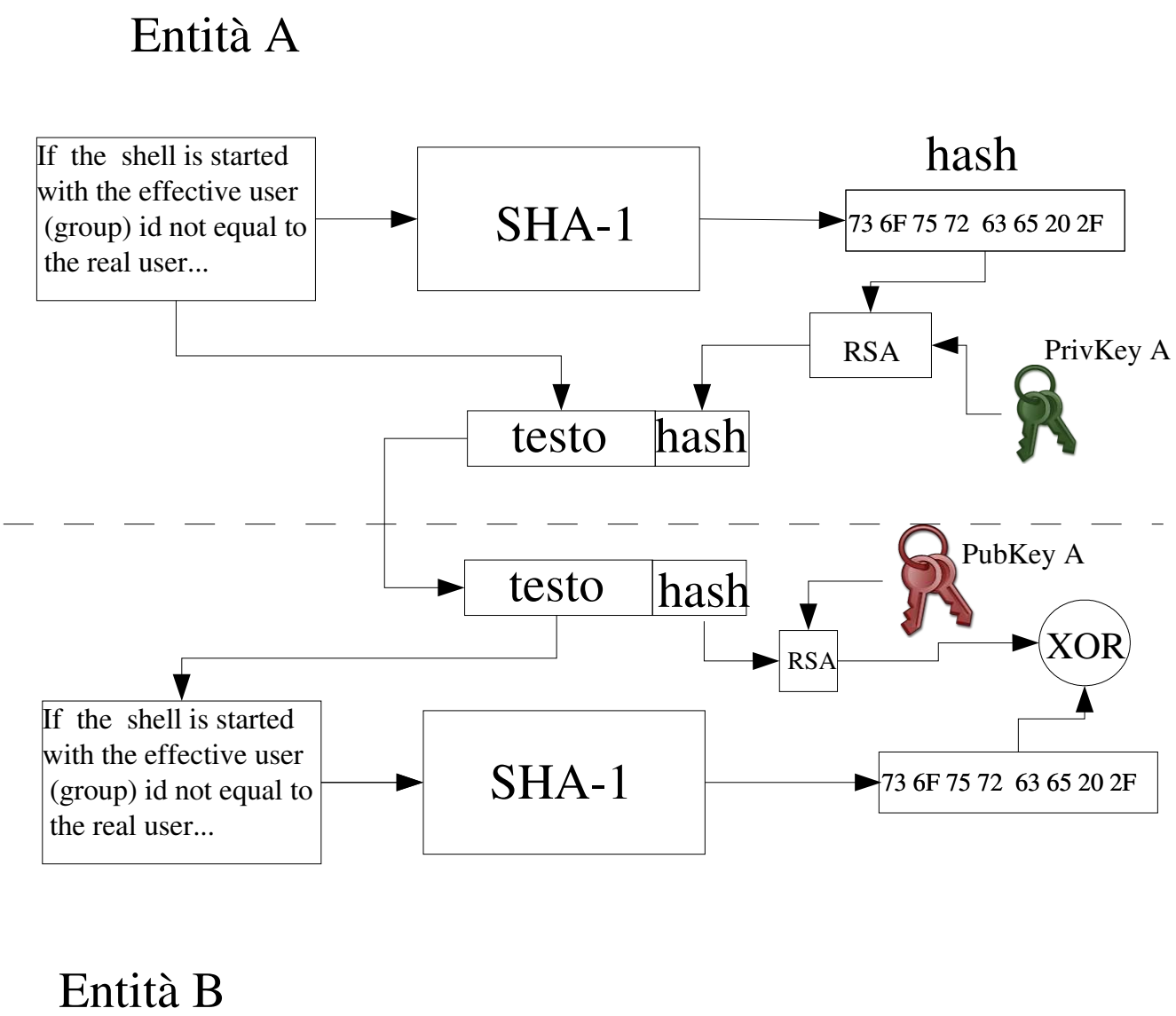
Firma digitale

- Le chiavi pubblica e privata sono invertibili
- Si può cifrare con la privata e decifrare con la pubblica
- Chi decifra è anche sicuro dell'identità del mittente

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Firma digitale



Principi di crittografia:
- Cifratura a chiave simmetrica
- Cifratura a chiave pubblica/privata
- Funzioni hash
- Certificati

Il protocollo 802.11i
- 802.1X e 802.11i
- Protocolli coinvolti
- Metodi EAP
- Protocolli di tunnel
- RADIUS vulnerability

WPA-PSK

Ente certificatrice

- Un ente che garantisce l'associazione tra chiave pubblica e persona fisica.
- L'ente possiede una sua coppia di chiavi pubblica/privata.
- Gli utenti conoscono l'ente (e la sua chiave pubblica) e si fidano delle certificazioni che rilascia.
- Alcuni enti di certificazione: Poste Italiane, Verisign ecc. . . .

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ente certificatrice

- Un ente che garantisce l'associazione tra chiave pubblica e persona fisica.
- L'ente possiede una sua coppia di chiavi pubblica/privata.
- Gli utenti conoscono l'ente (e la sua chiave pubblica) e si fidano delle certificazioni che rilascia.
- Alcuni enti di certificazione: Poste Italiane, Verisign ecc. . . .

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ente certificatrice

- Un ente che garantisce l'associazione tra chiave pubblica e persona fisica.
- L'ente possiede una sua coppia di chiavi pubblica/privata.
- Gli utenti conoscono l'ente (e la sua chiave pubblica) e si fidano delle certificazioni che rilascia.
- Alcuni enti di certificazione: Poste Italiane, Verisign ecc. . . .

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ente certificatrice

- Un ente che garantisce l'associazione tra chiave pubblica e persona fisica.
- L'ente possiede una sua coppia di chiavi pubblica/privata.
- Gli utenti conoscono l'ente (e la sua chiave pubblica) e si fidano delle certificazioni che rilascia.
- Alcuni enti di certificazione: Poste Italiane, Verisign ecc. . . .

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificazione

- Come avviene la certificazione:
  - L'utente A genera una coppia di chiavi pubblica/privata.
  - L'utente A invia all'ente la propria chiave pubblica, un documento.
  - L'ente restituisce la chiave pubblica dell'utente A firmata con la priopria chiave privata. Il contenitore in cui si sposta la chiave è un certificato.
  - Questa procedura si fa una sola volta, alla creazione della chiave.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificazione

- Come avviene la certificazione:
  - L'utente A genera una coppia di chiavi pubblica/privata.
  - L'utente A invia all'ente la propria chiave pubblica, un documento.
  - L'ente restituisce la chiave pubblica dell'utente A firmata con la priopria chiave privata. Il contenitore in cui si sposta la chiave è un certificato.
  - Questa procedura si fa una sola volta, alla creazione della chiave.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificazione

- Come avviene la certificazione:
  - L'utente A genera una coppia di chiavi pubblica/privata.
  - L'utente A invia all'ente la propria chiave pubblica, un documento.
  - L'ente restituisce la chiave pubblica dell'utente A firmata con la priopria chiave privata. Il contenitore in cui si sposta la chiave è un certificato.
  - Questa procedura si fa una sola volta, alla creazione della chiave.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificazione

- Come avviene la certificazione:
  - L'utente A genera una coppia di chiavi pubblica/privata.
  - L'utente A invia all'ente la propria chiave pubblica, un documento.
  - L'ente restituisce la chiave pubblica dell'utente A firmata con la priopria chiave privata. Il contenitore in cui si sposta la chiave è un certificato.
  - Questa procedura si fa una sola volta, alla creazione della chiave.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificazione

- Come avviene la certificazione:
  - L'utente A genera una coppia di chiavi pubblica/privata.
  - L'utente A invia all'ente la propria chiave pubblica, un documento.
  - L'ente restituisce la chiave pubblica dell'utente A firmata con la priopria chiave privata. Il contenitore in cui si sposta la chiave è un certificato.
  - Questa procedura si fa una sola volta, alla creazione della chiave.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificazione

- Quando un secondo utente B deve parlare con A, riceve il suo certificato,
- verifica la firma digitale dell'ente certificatrice,
- a quel punto è sicuro che l'utente A è davvero chi dichiara di essere, perchè l'ente certificatrice è testimone per lui.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificazione

- Quando un secondo utente B deve parlare con A, riceve il suo certificato,
- verifica la firma digitale dell'ente certificatrice,
- a quel punto è sicuro che l'utente A è davvero chi dichiara di essere, perchè l'ente certificatrice è testimone per lui.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificazione

- Quando un secondo utente B deve parlare con A, riceve il suo certificato,
- verifica la firma digitale dell'ente certificatrice,
- a quel punto è sicuro che l'utente A è davvero chi dichiara di essere, perchè l'ente certificatrice è testimone per lui.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificato digitale

Contiene:

- Dati identificativi dell'entità che fa da garante
- un serial number che identifica univocamente il certificato
- periodo di validità (da/a)
- dati identificativi del soggetto a cui è rilasciato (utente o dispositivo)
- la chiave pubblica del soggetto
- la firma digitale dell'ente che ha emesso il certificato

Identificatore entità di certificazione
Serial number
Periodo di validità
Dati soggetto
Chiave pubblica
Firma digitale dell'entità di certificazione

Certificato digitale

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificato digitale

Contiene:

- Dati identificativi dell'entità che fa da garante
- un serial number che identifica univocamente il certificato
- periodo di validità (da/a)
- dati identificativi del soggetto a cui è rilasciato (utente o dispositivo)
- la chiave pubblica del soggetto
- la firma digitale dell'ente che ha emesso il certificato

Identificatore entità di certificazione
Serial number
Periodo di validità
Dati soggetto
Chiave pubblica
Firma digitale dell'entità di certificazione

Certificato digitale

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificato digitale

Contiene:

- Dati identificativi dell'entità che fa da garante
- un serial number che identifica univocamente il certificato
- periodo di validità (da/a)
- dati identificativi del soggetto a cui è rilasciato (utente o dispositivo)
- la chiave pubblica del soggetto
- la firma digitale dell'ente che ha emesso il certificato

Identificatore entità di certificazione
Serial number
Periodo di validità
Dati soggetto
Chiave pubblica
Firma digitale dell'entità di certificazione

Certificato digitale

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificato digitale

Contiene:

- Dati identificativi dell'entità che fa da garante
- un serial number che identifica univocamente il certificato
- periodo di validità (da/a)
- dati identificativi del soggetto a cui è rilasciato (utente o dispositivo)
- la chiave pubblica del soggetto
- la firma digitale dell'ente che ha emesso il certificato

Identificatore entità di certificazione
Serial number
Periodo di validità
Dati soggetto
Chiave pubblica
Firma digitale dell'entità di certificazione

Certificato digitale

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificato digitale

Contiene:

- Dati identificativi dell'entità che fa da garante
- un serial number che identifica univocamente il certificato
- periodo di validità (da/a)
- dati identificativi del soggetto a cui è rilasciato (utente o dispositivo)
- la chiave pubblica del soggetto
- la firma digitale dell'ente che ha emesso il certificato

Identificatore entità di certificazione
Serial number
Periodo di validità
Dati soggetto
Chiave pubblica
Firma digitale dell'entità di certificazione

Certificato digitale

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Certificato digitale

Contiene:

- Dati identificativi dell'entità che fa da garante
- un serial number che identifica univocamente il certificato
- periodo di validità (da/a)
- dati identificativi del soggetto a cui è rilasciato (utente o dispositivo)
- la chiave pubblica del soggetto
- la firma digitale dell'ente che ha emesso il certificato

Identificatore entità di certificazione
Serial number
Periodo di validità
Dati soggetto
Chiave pubblica
Firma digitale dell'entità di certificazione

Certificato digitale

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Abbreviazioni:

802.1X	Port-Based Network Access Control standard.
WPA	Wireless Protected Access certification (vers. 1 o 2).
EAP	Extensible Authentication Protocol.
EAPoL	EAP Over LAN.
TLS	Transport Layer Security.
RADIUS	Remote Authentication Dial In User Service

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Storia di 802.11i

4/2003 Nasce WPA.

6/2004 Nasce lo standard 802.11i, quindi WPA2.

Molti produttori hanno rilasciato degli aggiornamenti di firmware/driver perchè i loro vecchi prodotti pre 802.11i fossero compatibili almeno con WPA.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Novità in 802.11i

- Algoritmi di crittografia rinnovati:
  - TKIP: utilizza sempre RC4 ma in una modalità che non permette gli attacchi visti su WEP
  - CCMP: abbandona RC4 e utilizza AES per la cifratura.
- Gestione delle chiavi rinnovata:

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Novità in 802.11i

- Algoritmi di crittografia rinnovati:
  - TKIP: utilizza sempre RC4 ma in una modalità che non permette gli attacchi visti su WEP
  - CCMP: abbandona RC4 e utilizza AES per la cifratura.
- Gestione delle chiavi rinnovata:
  - WPA PSK: AES-RC4 con chiavi condivise
  - 802.1X: usato authentication

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Novità in 802.11i

- Algoritmi di crittografia rinnovati:
  - TKIP: utilizza sempre RC4 ma in una modalità che non permette gli attacchi visti su WEP
  - CCMP: abbandona RC4 e utilizza AES per la cifratura.
- Gestione delle chiavi rinnovata:
  - WPA-PSK: pre-shared key tra macchine della rete.
  - 802.1X based authentication.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Novità in 802.11i

- Algoritmi di crittografia rinnovati:
  - TKIP: utilizza sempre RC4 ma in una modalità che non permette gli attacchi visti su WEP
  - CCMP: abbandona RC4 e utilizza AES per la cifratura.
- Gestione delle chiavi rinnovata:
  - WPA-PSK: pre-shared key tra macchine della rete.
  - 802.1X based authentication.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Novità in 802.11i

- Algoritmi di crittografia rinnovati:
  - TKIP: utilizza sempre RC4 ma in una modalità che non permette gli attacchi visti su WEP
  - CCMP: abbandona RC4 e utilizza AES per la cifratura.
- Gestione delle chiavi rinnovata:
  - WPA-PSK: pre-shared key tra macchine della rete.
  - 802.1X based authentication.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Novità in 802.11i

- Algoritmi di crittografia rinnovati:
  - TKIP: utilizza sempre RC4 ma in una modalità che non permette gli attacchi visti su WEP
  - CCMP: abbandona RC4 e utilizza AES per la cifratura.
- Gestione delle chiavi rinnovata:
  - WPA-PSK: pre-shared key tra macchine della rete.
  - 802.1X based authentication.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Cosa non cambia in 802.11i

- Il traffico di management.
- Il traffico di controllo.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Cosa non cambia in 802.11i

- Il traffico di management.
- Il traffico di controllo.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA e WPA2

- WPA è una versione di 802.11i che anticipa lo standard, utilizza gli algoritmi TKIP con gestione delle chiavi statica (detta anche WPA Home o WPA-PSK).
  - Gli AP o le schede client possono utilizzare TKIP con un semplice aggiornamento del firmware.
- WPA2 è la versione completa dello standard con l'utilizzo di 802.1X (WPA Enterprise).
  - Gli AP devono supportare AES-CCMP, TKIP è opzionale.
  - WPA2 Personal adotta AES-CCMP con chiavi statiche.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA e WPA2

- WPA è una versione di 802.11i che anticipa lo standard, utilizza gli algoritmi TKIP con gestione delle chiavi statica (detta anche WPA Home o WPA-PSK).
  - Gli AP o le schede client possono utilizzare TKIP con un semplice aggiornamento del firmware.
- WPA2 è la versione completa dello standard con l'utilizzo di 802.1X (WPA Enterprise).
  - Gli AP devono implementare i client RADIUS e l'algoritmo CCMP. Difficilmente realizzabile su hardware limitati.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA e WPA2

- WPA è una versione di 802.11i che anticipa lo standard, utilizza gli algoritmi TKIP con gestione delle chiavi statica (detta anche WPA Home o WPA-PSK).
  - Gli AP o le schede client possono utilizzare TKIP con un semplice aggiornamento del firmware.
- WPA2 è la versione completa dello standard con l'utilizzo di 802.1X (WPA Enterprise).
  - Gli AP devono implementare i client RADIUS e l'algoritmo CCMP. Difficilmente realizzabile su hardware limitati.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA e WPA2

- WPA è una versione di 802.11i che anticipa lo standard, utilizza gli algoritmi TKIP con gestione delle chiavi statica (detta anche WPA Home o WPA-PSK).
  - Gli AP o le schede client possono utilizzare TKIP con un semplice aggiornamento del firmware.
- WPA2 è la versione completa dello standard con l'utilizzo di 802.1X (WPA Enterprise).
  - Gli AP devono implementare i client RADIUS e l'algoritmo CCMP. Difficilmente realizzabile su hardware limitati.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

802.1x Port-Based Network Access Control

- É uno standard che definisce dei ruoli generici per l'architettura di controllo degli accessi in reti 802.
- Si dividono i due ruoli dell' *autenticator* e dell'AP, che offre semplicemente l'accesso di livello II.
- In questo modo si ridisegna la topologia della rete, rendendola meglio gestibile.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

802.1x Port-Based Network Access Control

- É uno standard che definisce dei ruoli generici per l'architettura di controllo degli accessi in reti 802.
- Si dividono i due ruoli dell' *autenticator* e dell'AP, che offre semplicemente l'accesso di livello II.
- In questo modo si ridisegna la topologia della rete, rendendola meglio gestibile.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

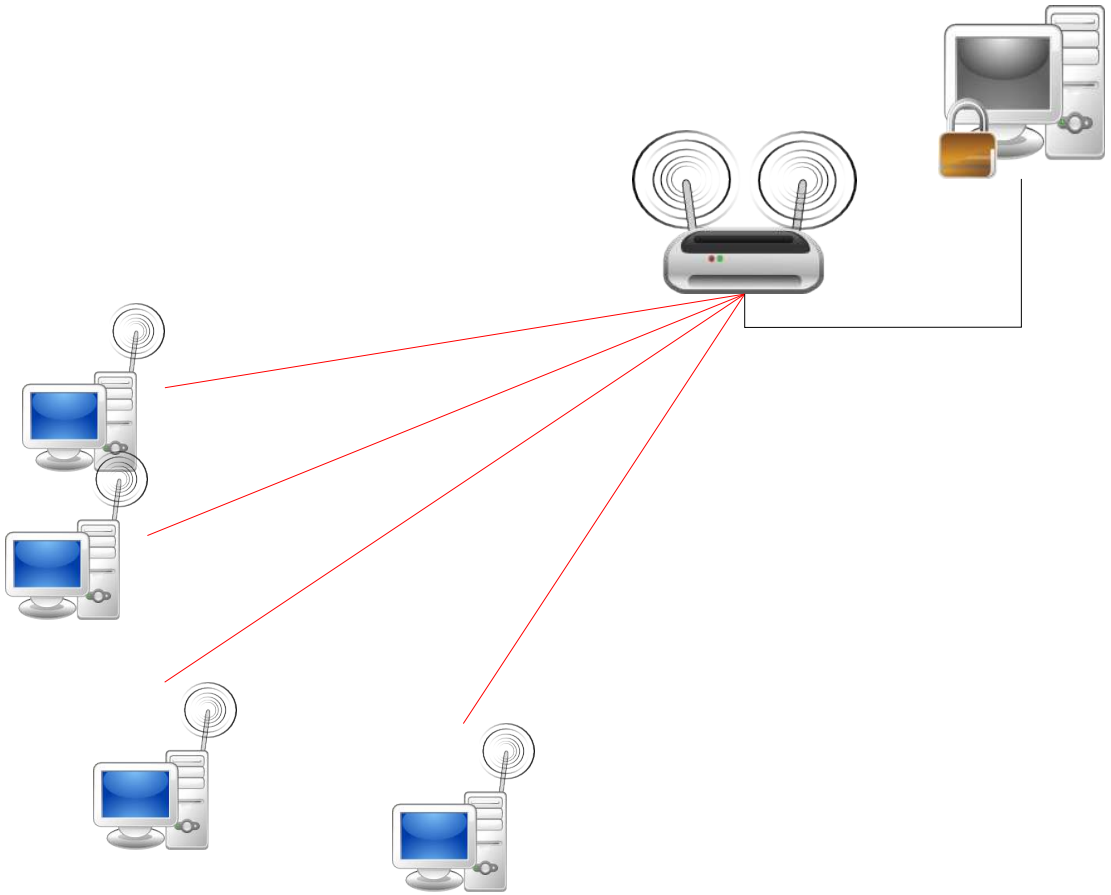
802.1x Port-Based Network Access Control

- É uno standard che definisce dei ruoli generici per l'architettura di controllo degli accessi in reti 802.
- Si dividono i due ruoli dell' *autenticator* e dell'AP, che offre semplicemente l'accesso di livello II.
- In questo modo si ridisegna la topologia della rete, rendendola meglio gestibile.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

802.1X - Topologia

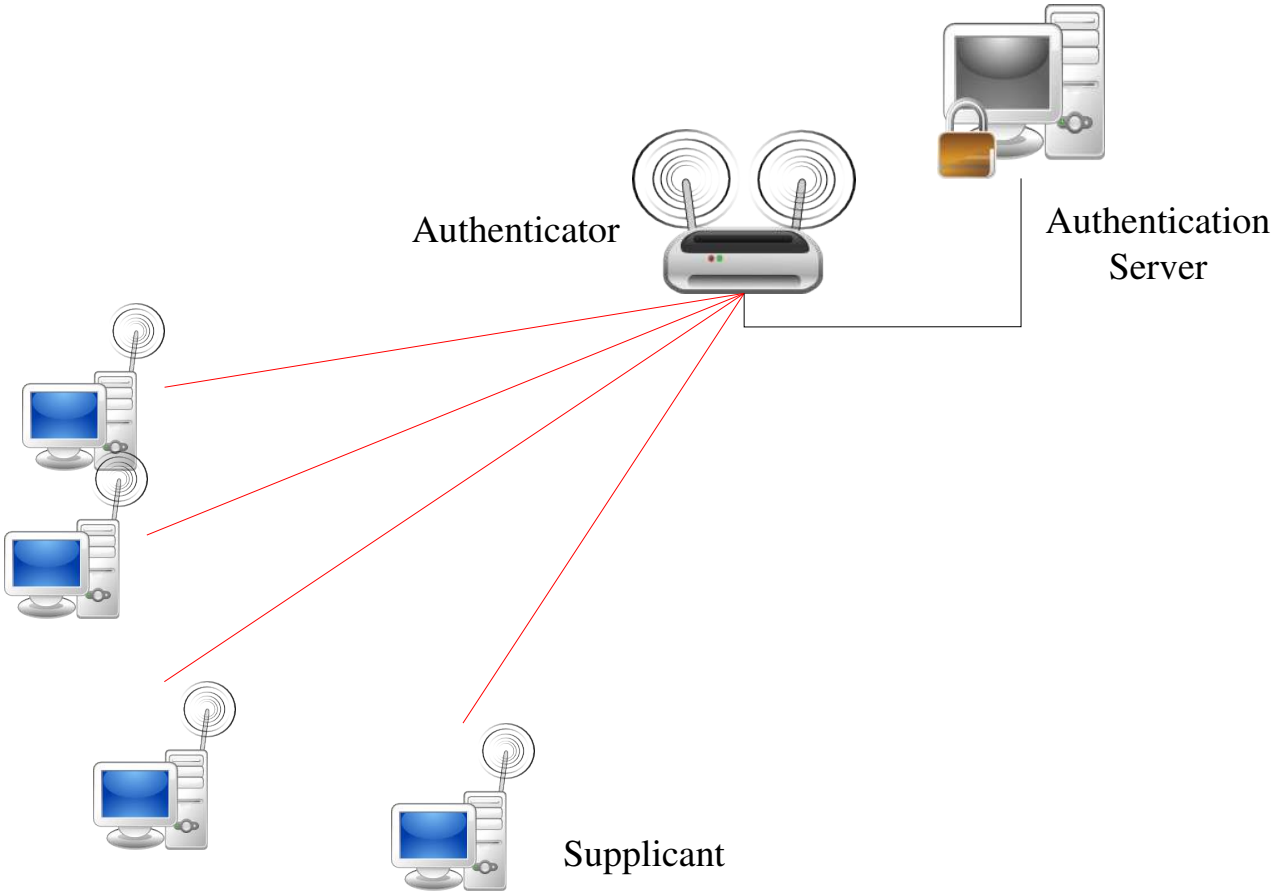


Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

802.1X - Topologia

I link in nero/spezzati sono wired, quelli in rosso/treggiati/diretti sono wireless. Il link tra *authenticator* e *authentication server* è un link che viene considerato sicuro ed è un link di livello >3



Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
- *authentication server*

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (passa i messaggi tra *supplicant* e *authentication server*).
  - Alla fine dell'autenticazione deve possedere una chiave condivisa con il *supplicant*.
  - Questa chiave deriva da quella generata dal server (per ragioni di sicurezza).
- *authentication server*

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (proxy).
  - Alla fine dell'atenticazione deve possedere del *keying matherial* in comune con il *supplicant*.
  - Quando riceve da supplicant le chiavi (pairwise e group) deve inoltrarle al AP.
- *authentication server*

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (proxy).
  - Alla fine dell'atenticazione deve possedere del *keying matherial* in comune con il *supplicant*.
  - Subito dopo deriva da questo delle chiavi per cifrare e autenticare.
- *authentication server*

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (proxy).
  - Alla fine dell'atenticazione deve possedere del *keying matherial* in comune con il *supplicant*.
  - Subito dopo deriva da questo delle chiavi per cifrare e autenticare.
- *authentication server*

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (proxy).
  - Alla fine dell'atenticazione deve possedere del *keying matherial* in comune con il *supplicant*.
  - Subito dopo deriva da questo delle chiavi per cifrare e autenticare.
- *authentication server*
  - Può essere [illegible] l'*authenticator*.
  - Si tratta di un [illegible] AAA.
  - Deve [illegible] *keying matherial* [illegible] *supplicant* [illegible] *authenticator*.
  - Spesso [illegible] EAP [illegible] 802.1X [illegible] RADIUS.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (proxy).
  - Alla fine dell'atenticazione deve possedere del *keying matherial* in comune con il *supplicant*.
  - Subito dopo deriva da questo delle chiavi per cifrare e autenticare.
- *authentication server*
  - É un database di credenziali di autenticazione, quindi è lui che autentica il *supplicant*.
  - Una volta stabilità l'identità di *supplicant* decide se farlo entrare o meno e lo comunica all'*authenticator*.
  - Anche quando il supplicant si sposta da un access point all'altro, l'authenticator deve essere sempre lo stesso.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (proxy).
  - Alla fine dell'atenticazione deve possedere del *keying matherial* in comune con il *supplicant*.
  - Subito dopo deriva da questo delle chiavi per cifrare e autenticare.
- *authentication server*
  - É un database di credenziali di autenticazione, quindi è lui che autentica il *supplicant*.
  - Una volta stabilità l'identità di *supplicant* decide se farlo entrare o meno e lo comunica all'*authenticator*.
  - Anche l'*authentication server* si deve autenticare con il *supplicant*, l'autenticazione è sempre bidirezionale.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (proxy).
  - Alla fine dell'atenticazione deve possedere del *keying matherial* in comune con il *supplicant*.
  - Subito dopo deriva da questo delle chiavi per cifrare e autenticare.
- *authentication server*
  - É un database di credenziali di autenticazione, quindi è lui che autentica il *supplicant*.
  - Una volta stabilità l'identità di *supplicant* decide se farlo entrare o meno e lo comunica all'*authenticator*.
  - Anche l'*authentication server* si deve autenticare con il *supplicant*, l'autenticazione è sempre bidirezionale.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (proxy).
  - Alla fine dell'atenticazione deve possedere del *keying matherial* in comune con il *supplicant*.
  - Subito dopo deriva da questo delle chiavi per cifrare e autenticare.
- *authentication server*
  - É un database di credenziali di autenticazione, quindi è lui che autentica il *supplicant*.
  - Una volta stabilità l'identità di *supplicant* decide se farlo entrare o meno e lo comunica all'*authenticator*.
  - Anche l'*authentication server* si deve autenticare con il *supplicant*, l'autenticazione è sempre bidirezionale.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Ruoli

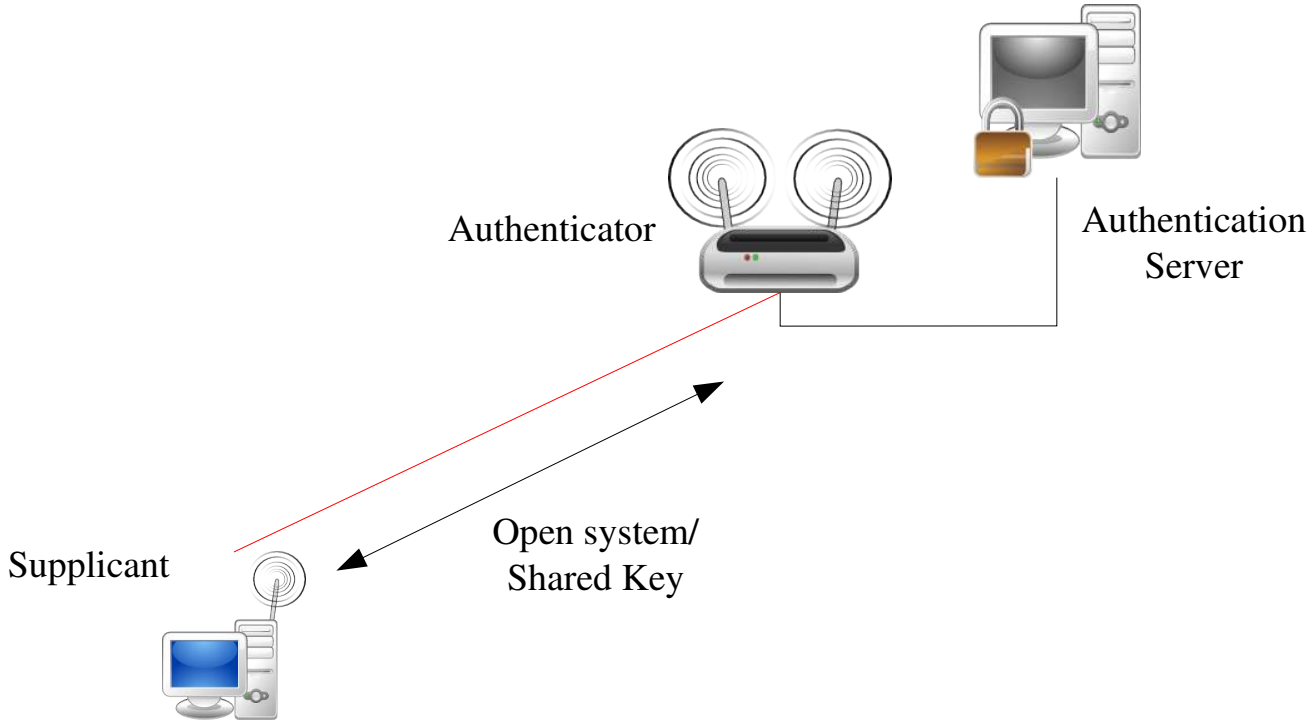
- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (proxy).
  - Alla fine dell'atenticazione deve possedere del *keying matherial* in comune con il *supplicant*.
  - Subito dopo deriva da questo delle chiavi per cifrare e autenticare.
- *authentication server*
  - É un database di credenziali di autenticazione, quindi è lui che autentica il *supplicant*.
  - Una volta stabilità l'identità di *supplicant* decide se farlo entrare o meno e lo comunica all'*authenticator*.
  - Anche l'*authentication server* si deve autenticare con il *supplicant*, l'autenticazione è sempre bidirezionale.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Fasi

Prima fase: autenticazione 802.11 (solo per compatibilità) e associazione.



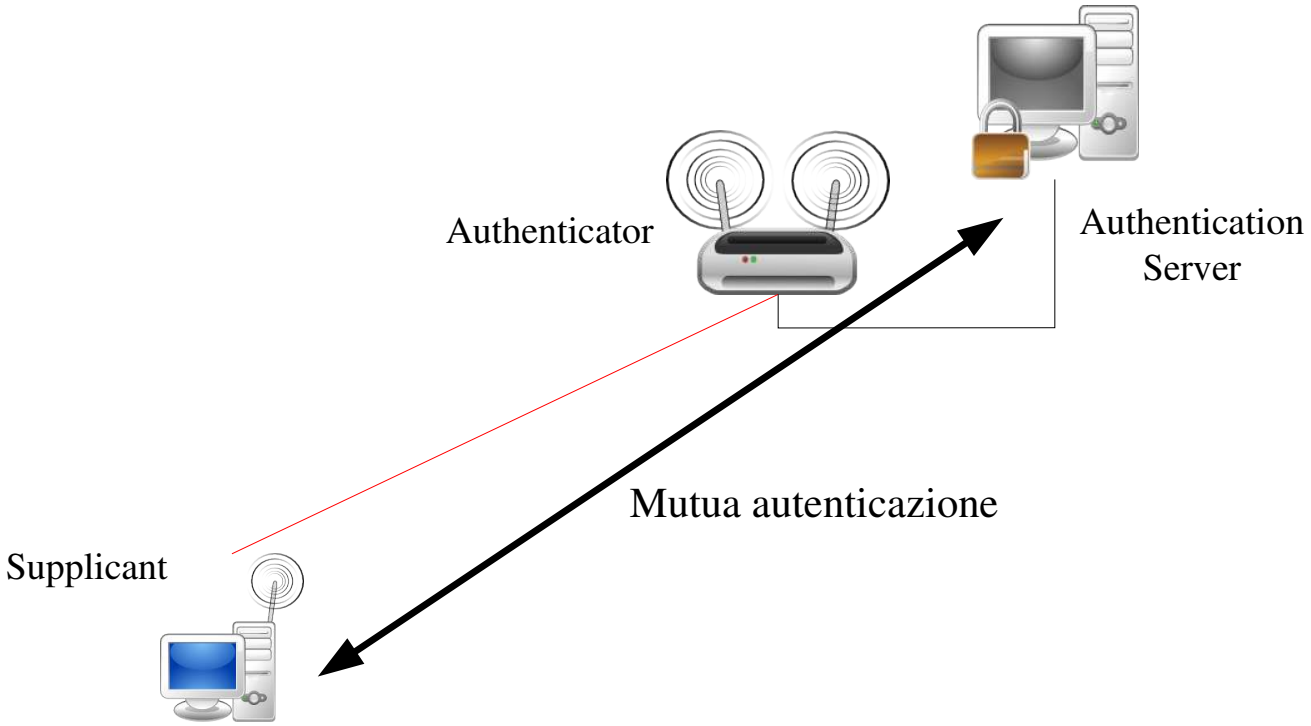
Principi di crittografia:
- Cifratura a chiave simmetrica
- Cifratura a chiave pubblica/privata
- Funzioni hash
- Certificati

Il protocollo 802.11i
- 802.1X e 802.11i
- Protocolli coinvolti
- Metodi EAP
- Protocolli di tunnel
- RADIUS vulnerability

WPA-PSK

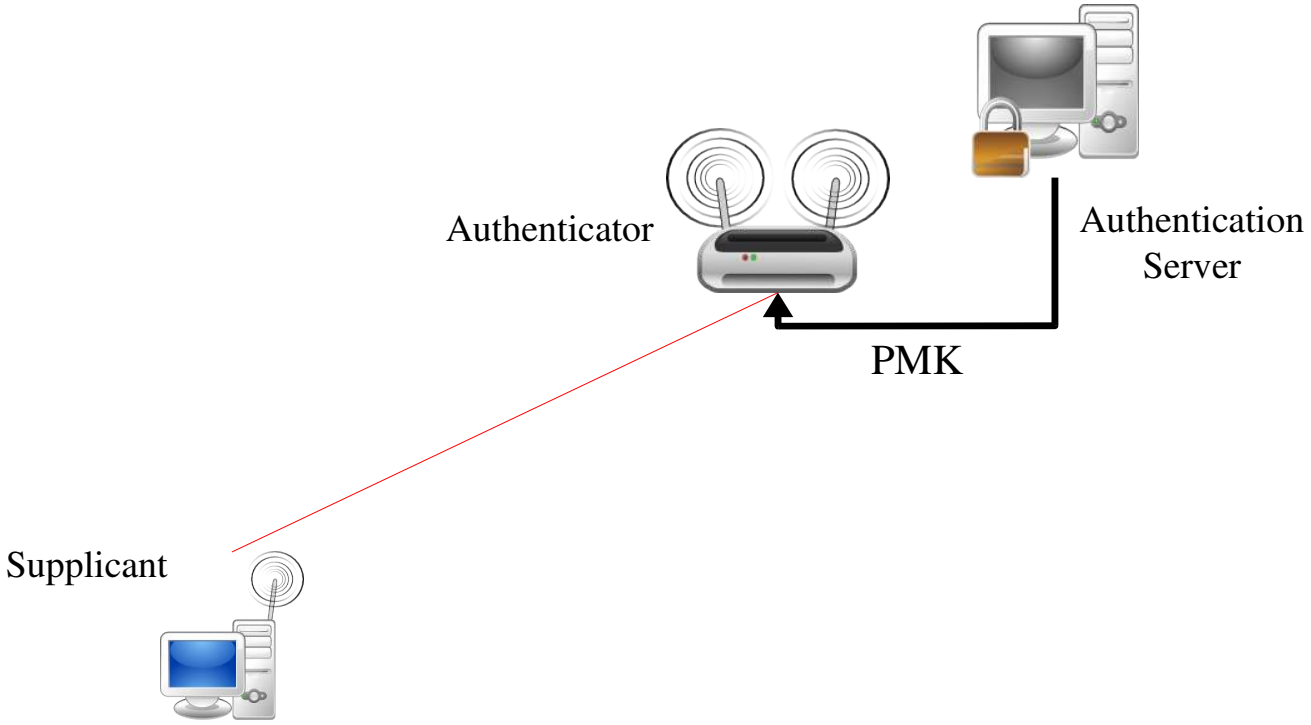
Fasi

Seconda fase: autenticazione tra *supplicant* e *authentication server*. Le due macchine verificano la reciproca identità e producono una chiave simmetrica PMK (Pairwise master key).



Fasi

Terza fase: la PMK viene spostata sull'*authenticator*.

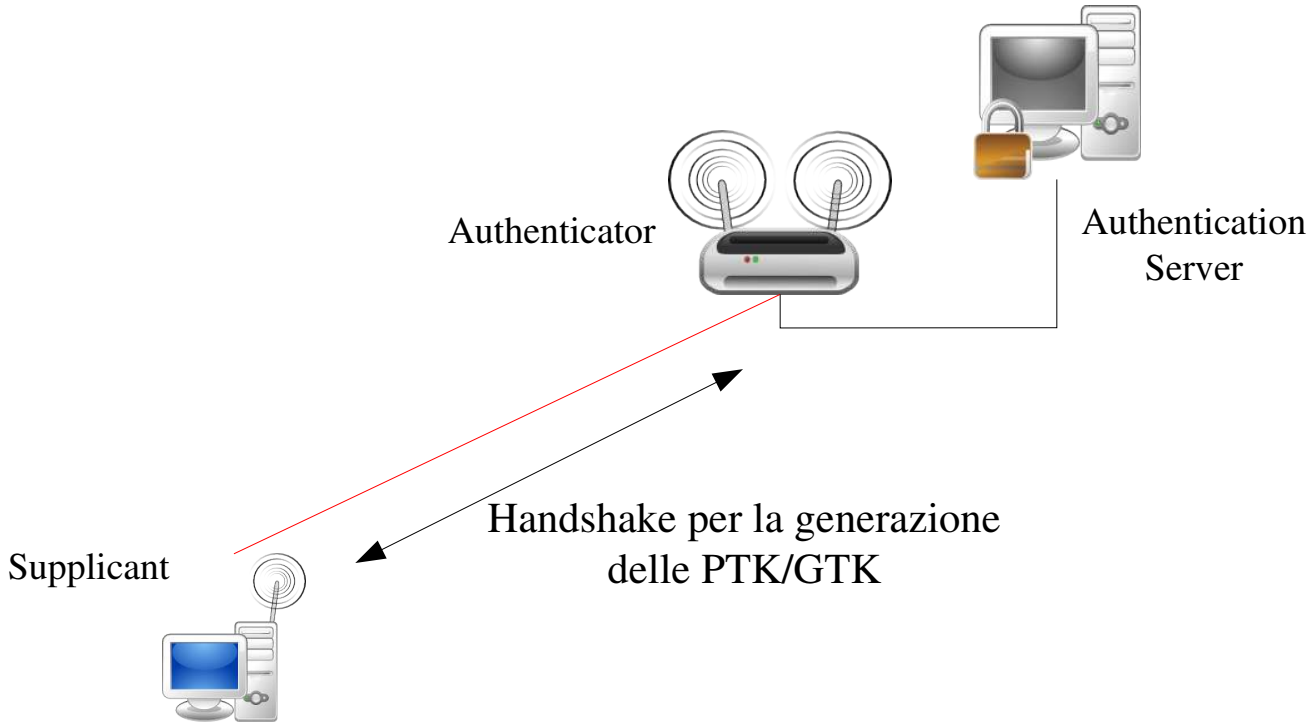


Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Fasi

Quarta fase: a partire dalla PMK *supplicant* e *authenticator* derivano delle chiavi che verranno utilizzate per cifrare e autenticare tutti i pacchetti successivi (chiave PTK per il traffico unicast e GTK per il traffico broadcast).



Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

- Da questo momento in poi l'*authentication server* non partecipa più alle comunicazioni se non interpellato. Saltuariamente *supplicant* e *authenticator* possono decidere di generare delle nuove GTK e PTK a partire dalla PMK che rimane la stessa (key *refresh*).
- L'*authenticator* può decidere di forzare anche una riautenticazione, e costringere il *supplicant* a ripetere l'autenticazione iniziale per generare una nuova chiave PMK.
- Un'autenticazione completa coinvolge diversi protocolli e può essere configurata in molti modi diversi.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

- Da questo momento in poi l'*authentication server* non partecipa più alle comunicazioni se non interpellato. Saltuariamente *supplicant* e *authenticator* possono decidere di generare delle nuove GTK e PTK a partire dalla PMK che rimane la stessa (key *refresh*).
- L'*authenticator* può decidere di forzare anche una riautenticazione, e costringere il *supplicant* a ripetere l'autenticazione iniziale per generare una nuova chiave PMK.
- Un'autenticazione completa coinvolge diversi protocolli e può essere configurata in molti modi diversi.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

- Da questo momento in poi l'*authentication server* non partecipa più alle comunicazioni se non interpellato. Saltuariamente *supplicant* e *authenticator* possono decidere di generare delle nuove GTK e PTK a partire dalla PMK che rimane la stessa (key *refresh*).
- L'*authenticator* può decidere di forzare anche una riautenticazione, e costringere il *supplicant* a ripetere l'autenticazione iniziale per generare una nuova chiave PMK.
- Un'autenticazione completa coinvolge diversi protocolli e può essere configurata in molti modi diversi.

Protocolli utilizzati:

I protocolli possono essere di due tipi:

- End to End (ete): un protocollo che coinvolge due macchine virtualmente collegate, ma non fisicamente comunicanti (ad es. TCP/UDP). Nel nostro caso EAP.
- Point to Point (ptp): un protocollo che coinvolge due macchine che sono direttamente connesse (ad es. DHCP). Nel nostro caso EAPoL, ma anche, astrattamente RADIUS.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli utilizzati:

I protocolli possono essere di due tipi:

- End to End (ete): un protocollo che coinvolge due macchine virtualmente collegate, ma non fisicamente comunicanti (ad es. TCP/UDP). Nel nostro caso EAP.
- Point to Point (ptp): un protocollo che coinvolge due macchine che sono direttamente connesse (ad es. DHCP). Nel nostro caso EAPoL, ma anche, astrattamente RADIUS.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli utilizzati:

Fase 1: Standard 802.11a/b/g.

Fase 2: Tra *supplicant* e *authentication server* si usa il protocollo EAP (ete). Questo viene veicolato tra *supplicant* e *authenticator* dentro a pacchetti in formato EAPoL, e tra *authenticator* e *authentication server* attraverso il protocollo RADIUS (ptp).

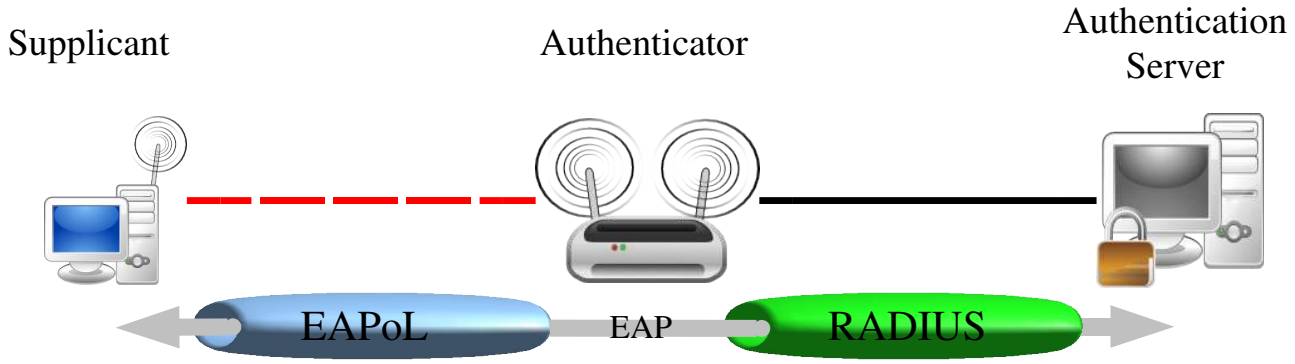
Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli utilizzati:

Fase 1: Standard 802.11a/b/g.

Fase 2: Tra *supplicant* e *authentication server* si usa il protocollo EAP (ete). Questo viene veicolato tra *supplicant* e *authenticator* dentro a pacchetti in formato EAPoL, e tra *authenticator* e *authentication server* attraverso il protocollo RADIUS (ptp).



Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli utilizzati:

Fase 3: La chiave viene spostata con il protocollo RADIUS.

Fase 4: La generazione di PTK/GTK viene realizzata con un handshake definito in 802.11i.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli utilizzati:

Fase 3: La chiave viene spostata con il protocollo RADIUS.

Fase 4: La generazione di PTK/GTK viene realizzata con un handshake definito in 802.11i.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- EAP è un protocollo di *trasporto* di meccanismi generici di autenticazione tra due *peer*. Da solo non realizza nessuna autenticazione, ma dentro ad EAP possono essere veicolati dei *metodi di autenticazione* specifici:
  - TLS
  - MD5
  - TTLS
  - ...
- Alcuni di questi meccanismi producono:
- Lo standard 802.11i obbliga ad utilizzare un metodo EAP che garantisca entrambe le caratteristiche precedenti (ad es. TLS, non MD5).

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- EAP è un protocollo di *trasporto* di meccanismi generici di autenticazione tra due *peer*. Da solo non realizza nessuna autenticazione, ma dentro ad EAP possono essere veicolati dei *metodi di autenticazione* specifici:
  - TLS
  - MD5
  - TTLS
  - ...
- Alcuni di questi meccanismi producono:
- Lo standard 802.11i obbliga ad utilizzare un metodo EAP che garantisca entrambe le caratteristiche precedenti (ad es. TLS, non MD5).

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- EAP è un protocollo di *trasporto* di meccanismi generici di autenticazione tra due *peer*. Da solo non realizza nessuna autenticazione, ma dentro ad EAP possono essere veicolati dei *metodi di autenticazione* specifici:
  - TLS
  - MD5
  - TTLS
  - ...
- Alcuni di questi meccanismi producono:
- Lo standard 802.11i obbliga ad utilizzare un metodo EAP che garantisca entrambe le caratteristiche precedenti (ad es. TLS, non MD5).

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- EAP è un protocollo di *trasporto* di meccanismi generici di autenticazione tra due *peer*. Da solo non realizza nessuna autenticazione, ma dentro ad EAP possono essere veicolati dei *metodi di autenticazione* specifici:
  - TLS
  - MD5
  - TTLS
  - ...
- Alcuni di questi meccanismi producono:
  - una chiave autenticata tra i due peer
  - una chiave che viene usata per cifrare il traffico successivo
- Lo standard 802.11i obbliga ad utilizzare un metodo EAP che garantisca entrambe le caratteristiche precedenti (ad es. TLS, non MD5).

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- EAP è un protocollo di *trasporto* di meccanismi generici di autenticazione tra due *peer*. Da solo non realizza nessuna autenticazione, ma dentro ad EAP possono essere veicolati dei *metodi di autenticazione* specifici:
  - TLS
  - MD5
  - TTLS
  - ...
- Alcuni di questi meccanismi producono:
  - mutua autenticazione tra i due peer.
  - *generazione* di *keying material* da riutilizzare successivamente.
- Lo standard 802.11i obbliga ad utilizzare un metodo EAP che garantisca entrambe le caratteristiche precedenti (ad es. TLS, non MD5).

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- EAP è un protocollo di *trasporto* di meccanismi generici di autenticazione tra due *peer*. Da solo non realizza nessuna autenticazione, ma dentro ad EAP possono essere veicolati dei *metodi di autenticazione* specifici:
  - TLS
  - MD5
  - TTLS
  - ...
- Alcuni di questi meccanismi producono:
  - mutua autenticazione tra i due peer.
  - generazione di *keying matherial* da riutilizzare successivamente.
- Lo standard 802.11i obbliga ad utilizzare un metodo EAP che garantisca entrambe le caratteristiche precedenti (ad es. TLS, non MD5).

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- EAP è un protocollo di *trasporto* di meccanismi generici di autenticazione tra due *peer*. Da solo non realizza nessuna autenticazione, ma dentro ad EAP possono essere veicolati dei *metodi di autenticazione* specifici:
  - TLS
  - MD5
  - TTLS
  - ...
- Alcuni di questi meccanismi producono:
  - mutua autenticazione tra i due peer.
  - generazione di *keying matherial* da riutilizzare successivamente.
- Lo standard 802.11i obbliga ad utilizzare un metodo EAP che garantisca entrambe le caratteristiche precedenti (ad es. TLS, non MD5).

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- EAP è un protocollo di *trasporto* di meccanismi generici di autenticazione tra due *peer*. Da solo non realizza nessuna autenticazione, ma dentro ad EAP possono essere veicolati dei *metodi di autenticazione* specifici:
  - TLS
  - MD5
  - TTLS
  - ...
- Alcuni di questi meccanismi producono:
  - mutua autenticazione tra i due peer.
  - generazione di *keying matherial* da riutilizzare successivamente.
- Lo standard 802.11i obbliga ad utilizzare un metodo EAP che garantisca entrambe le caratteristiche precedenti (ad es. TLS, non MD5).

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- EAP è un protocollo di *trasporto* di meccanismi generici di autenticazione tra due *peer*. Da solo non realizza nessuna autenticazione, ma dentro ad EAP possono essere veicolati dei *metodi di autenticazione* specifici:
  - TLS
  - MD5
  - TTLS
  - ...
- Alcuni di questi meccanismi producono:
  - mutua autenticazione tra i due peer.
  - generazione di *keying matherial* da riutilizzare successivamente.
- Lo standard 802.11i obbliga ad utilizzare un metodo EAP che garantisca entrambe le caratteristiche precedenti (ad es. TLS, non MD5).

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- Anche RADIUS è un protocollo di *trasporto* di meccanismi di autenticazione, ma può veicolare anche altri contenuti (RADIUS è un protocollo AAA: Authentication, Authorization and Accounting) che si basa su un modello client/server. Anche RADIUS è uno scheletro per veicolare singoli *attributi RADIUS* che compiono scopi specifici.
  - Attributo EAP: RADIUS è in grado di veicolare pacchetti EAP, e contiene al suo interno lo stack protocollare di EAP, compresi i metodi specifici.
  - ...
- RADIUS rende sicuro il canale tra *authentication server* e *authenticator* utilizzando una chiave segreta. La chiave serve al client per poter fare richieste e ai singoli attributi per cifrare/autenticare le richieste.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- Anche RADIUS è un protocollo di *trasporto* di meccanismi di autenticazione, ma può veicolare anche altri contenuti (RADIUS è un protocollo AAA: Authentication, Authorization and Accounting) che si basa su un modello client/server. Anche RADIUS è uno scheletro per veicolare singoli *attributi RADIUS* che compiono scopi specifici.
  - Attributo EAP: RADIUS è in grado di veicolare pacchetti EAP, e contiene al suo interno lo stack protocollare di EAP, compresi i metodi specifici.
  - ...
- RADIUS rende sicuro il canale tra *authentication server* e *authenticator* utilizzando una chiave segreta. La chiave serve al client per poter fare richieste e ai singoli attributi per cifrare/autenticare le richieste.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- Anche RADIUS è un protocollo di *trasporto* di meccanismi di autenticazione, ma può veicolare anche altri contenuti (RADIUS è un protocollo AAA: Authentication, Authorization and Accounting) che si basa su un modello client/server. Anche RADIUS è uno scheletro per veicolare singoli *attributi RADIUS* che compiono scopi specifici.
  - Attributo EAP: RADIUS è in grado di veicolare pacchetti EAP, e contiene al suo interno lo stack protocollare di EAP, compresi i metodi specifici.
  - ...
- RADIUS rende sicuro il canale tra *authentication server* e *authenticator* utilizzando una chiave segreta. La chiave serve al client per poter fare richieste e ai singoli attributi per cifrare/autenticare le richieste.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Protocolli modulari:

- Anche RADIUS è un protocollo di *trasporto* di meccanismi di autenticazione, ma può veicolare anche altri contenuti (RADIUS è un protocollo AAA: Authentication, Authorization and Accounting) che si basa su un modello client/server. Anche RADIUS è uno scheletro per veicolare singoli *attributi RADIUS* che compiono scopi specifici.
  - Attributo EAP: RADIUS è in grado di veicolare pacchetti EAP, e contiene al suo interno lo stack protocollare di EAP, compresi i metodi specifici.
  - ...
- RADIUS rende sicuro il canale tra *authentication server* e *authenticator* utilizzando una chiave segreta. La chiave serve al client per poter fare richieste e ai singoli attributi per cifrare/autenticare le richieste.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Incapsulamento dei pacchetti

- I pacchetti EAP vengono creati dal *supplicant* e vengono inseriti in un frame EAPoL.
- Quando arrivano all'*authenticator* gli viene tolto l'header EAPoL e vengono reincapsulati in un pacchetto RADIUS.
- Il procedimento opposto viene prodotto quando il pacchetto torna indietro dall' *authentication server* all'*authenticator*.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Incapsulamento dei pacchetti

- I pacchetti EAP vengono creati dal *supplicant* e vengono inseriti in un frame EAPoL.
- Quando arrivano all'*authenticator* gli viene tolto l'header EAPoL e vengono reincapsulati in un pacchetto RADIUS.
- Il procedimento opposto viene prodotto quando il pacchetto torna indietro dall' *authentication server* all'*authenticator*.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Incapsulamento dei pacchetti

- I pacchetti EAP vengono creati dal *supplicant* e vengono inseriti in un frame EAPoL.
- Quando arrivano all'*authenticator* gli viene tolto l'header EAPoL e vengono reincapsulati in un pacchetto RADIUS.
- Il procedimento opposto viene prodotto quando il pacchetto torna indietro dall' *authentication server* all'*authenticator*.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- É la versione per EAP del protocollo TLS:
  - Basato su chiave pubblica/privata e certificati.
  - Permette la mutua autenticazione dei partecipanti.
  - Alla fine della procedura di autenticazione entrambe le parti hanno anche generato una chiave simmetrica, in modo comune, senza che questa abbia attraversato la rete.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- É la versione per EAP del protocollo TLS:
  - Basato su chiave pubblica/privata e certificati.
  - Permette la mutua autenticazione dei partecipanti.
  - Alla fine della procedura di autenticazione entrambe le parti hanno anche generato una chiave simmetrica, in modo comune, senza che questa abbia attraversato la rete.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- É la versione per EAP del protocollo TLS:
  - Basato su chiave pubblica/privata e certificati.
  - Permette la mutua autenticazione dei partecipanti.
  - Alla fine della procedura di autenticazione entrambe le parti hanno anche generato una chiave simmetrica, in modo comune, senza che questa abbia attraversato la rete.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- É la versione per EAP del protocollo TLS:
  - Basato su chiave pubblica/privata e certificati.
  - Permette la mutua autenticazione dei partecipanti.
  - Alla fine della procedura di autenticazione entrambe le parti hanno anche generato una chiave simmetrica, in modo comune, senza che questa abbia attraversato la rete.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- Nel primo pacchetto dello scambio il *supplicant* invia all'*authentication server* il suo certificato digitale.
- Nel secondo l'*authentication server* invia il suo certificato.
- In questo modo entrabi verificano l'identità dell'altro.
- L'*authentication server* può decidere se permettere l'ingresso nella rete del *supplicant* basandosi sulla conoscenza della sua chiave pubblica, o sulla certificazione che il *supplicant* presenta.
- Se ci si basa sulle certificazioni, si possono rilasciare autorizzazioni temporanee, personali, non legate alla macchina ma all'utente in modo molto flessibile.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- Nel primo pacchetto dello scambio il *supplicant* invia all'*authentication server* il suo certificato digitale.
- Nel secondo l'*authentication server* invia il suo certificato.
- In questo modo entrabi verificano l'identità dell'altro.
- L'*authentication server* può decidere se permettere l'ingresso nella rete del *supplicant* basandosi sulla conoscenza della sua chiave pubblica, o sulla certificazione che il *supplicant* presenta.
- Se ci si basa sulle certificazioni, si possono rilasciare autorizzazioni temporanee, personali, non legate alla macchina ma all'utente in modo molto flessibile.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- Nel primo pacchetto dello scambio il *supplicant* invia all'*authentication server* il suo certificato digitale.
- Nel secondo l'*authentication server* invia il suo certificato.
- In questo modo entrabi verificano l'identità dell'altro.
- L'*authentication server* può decidere se permettere l'ingresso nella rete del *supplicant* basandosi sulla conoscenza della sua chiave pubblica, o sulla certificazione che il *supplicant* presenta.
- Se ci si basa sulle certificazioni, si possono rilasciare autorizzazioni temporanee, personali, non legate alla macchina ma all'utente in modo molto flessibile.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- Nel primo pacchetto dello scambio il *supplicant* invia all'*authentication server* il suo certificato digitale.
- Nel secondo l'*authentication server* invia il suo certificato.
- In questo modo entrabi verificano l'identità dell'altro.
- L'*authentication server* può decidere se permettere l'ingresso nella rete del *supplicant* basandosi sulla conoscenza della sua chiave pubblica, o sulla certificazione che il *supplicant* presenta.
- Se ci si basa sulle certificazioni, si possono rilasciare autorizzazioni temporanee, personali, non legate alla macchina ma all'utente in modo molto flessibile.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- Nel primo pacchetto dello scambio il *supplicant* invia all'*authentication server* il suo certificato digitale.
- Nel secondo l'*authentication server* invia il suo certificato.
- In questo modo entrabi verificano l'identità dell'altro.
- L'*authentication server* può decidere se permettere l'ingresso nella rete del *supplicant* basandosi sulla conoscenza della sua chiave pubblica, o sulla certificazione che il *supplicant* presenta.
- Se ci si basa sulle certificazioni, si possono rilasciare autorizzazioni temporanee, personali, non legate alla macchina ma all'utente in modo molto flessibile.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- Per ottenere l'autenticazione basata su certificati bisogna configurare il server RADIUS con:
  - il certificato dell'ente certificatrice.
  - il proprio certificato, firmato dall'ente certificatrice.
- Quando si riceve il certificato del client si verifica la sua validità utilizzando quello dell'ente certificatrice. Se il certificato non è valido l'autenticazione non va avanti.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- Per ottenere l'autenticazione basata su certificati bisogna configurare il server RADIUS con:
  - il certificato dell'ente certificatrice.
  - il proprio certificato, firmato dall'ente certificatrice.
- Quando si riceve il certificato del client si verifica la sua validità utilizzando quello dell'ente certificatrice. Se il certificato non è valido l'autenticazione non va avanti.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- Per ottenere l'autenticazione basata su certificati bisogna configurare il server RADIUS con:
  - il certificato dell'ente certificatrice.
  - il proprio certificato, firmato dall'ente certificatrice.
- Quando si riceve il certificato del client si verifica la sua validità utilizzando quello dell'ente certificatrice. Se il certificato non è valido l'autenticazione non va avanti.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- Per ottenere l'autenticazione basata su certificati bisogna configurare il server RADIUS con:
  - il certificato dell'ente certificatrice.
  - il proprio certificato, firmato dall'ente certificatrice.
- Quando si riceve il certificato del client si verifica la sua validità utilizzando quello dell'ente certificatrice. Se il certificato non è valido l'autenticazione non va avanti.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- TLS è progettato in modo da essere robusto contro attacchi di tipo man in the middle, ammesso che i due peer conoscano in precedenza le rispettive chiavi pubbliche. Se si utilizzano certificati invece l'ente certificatrice deve essere fidata. . .
- . . . se l'ente certificatrice rilascia certificati:
  - a scadenza infinita,
  - senza indicazioni *precise* dell'utente. . .
- . . . l'autenticazione può essere raggirata.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- TLS è progettato in modo da essere robusto contro attacchi di tipo man in the middle, ammesso che i due peer conoscano in precedenza le rispettive chiavi pubbliche. Se si utilizzano certificati invece l'ente certificatrice deve essere fidata. . .
- . . . se l'ente certificatrice rilascia certificati:
  - a scadenza infinita,
  - senza indicazioni precise dell'utente. . .
- . . . l'autenticazione può essere raggirata.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- TLS è progettato in modo da essere robusto contro attacchi di tipo man in the middle, ammesso che i due peer conoscano in precedenza le rispettive chiavi pubbliche. Se si utilizzano certificati invece l'ente certificatrice deve essere fidata. . .
- . . . se l'ente certificatrice rilascia certificati:
  - a scadenza infinita,
  - senza indicazioni precise dell'utente. . .
- . . . l'autenticazione può essere raggirata.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- TLS è progettato in modo da essere robusto contro attacchi di tipo man in the middle, ammesso che i due peer conoscano in precedenza le rispettive chiavi pubbliche. Se si utilizzano certificati invece l'ente certificatrice deve essere fidata. . .
- . . . se l'ente certificatrice rilascia certificati:
  - a scadenza infinita,
  - senza indicazioni precise dell'utente. . .
- . . . l'autenticazione può essere raggirata.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TLS

- TLS è progettato in modo da essere robusto contro attacchi di tipo man in the middle, ammesso che i due peer conoscano in precedenza le rispettive chiavi pubbliche. Se si utilizzano certificati invece l'ente certificatrice deve essere fidata. . .
- . . . se l'ente certificatrice rilascia certificati:
  - a scadenza infinita,
  - senza indicazioni precise dell'utente. . .
- . . . l'autenticazione può essere raggirata.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Tunneled EAP

- EAP-TLS richiede espressamente che entrambe le parti si autentichino con dei certificati digitali, il che non è facilmente implementabile (poco *user friendly*).
- Esistono altri metodi per poter autenticare un utente su un database, di cui il più semplice è la coppia User/Passwd.
  - MD5
  - MSCHAP
  - LEAP
  - ...
- Il problema di questi metodi è che possono subire attacchi di brute force anche offline, o attacchi reply, essendo crittograficamente piuttosto semplici.
- Si preferisce allora instaurare prima un tunnel TLS, e dentro al tunnel far passare le autenticazioni baste su User/Passwd.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Tunneled EAP

- EAP-TLS richiede espressamente che entrambe le parti si autentichino con dei certificati digitali, il che non è facilmente implementabile (poco *user friendly*).
- Esistono altri metodi per poter autenticare un utente su un database, di cui il più semplice è la coppia User/Passwd.
  - MD5
  - MSCHAP
  - LEAP
  - ...
- Il problema di questi metodi è che possono subire attacchi di brute force anche offline, o attacchi reply, essendo crittograficamente piuttosto semplici.
- Si preferisce allora instaurare prima un tunnel TLS, e dentro al tunnel far passare le autenticazioni baste su User/Passwd.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Tunneled EAP

- EAP-TLS richiede espressamente che entrambe le parti si autentichino con dei certificati digitali, il che non è facilmente implementabile (poco *user friendly*).
- Esistono altri metodi per poter autenticare un utente su un database, di cui il più semplice è la coppia User/Passwd.
  - MD5
  - MSCHAP
  - LEAP
  - ...
- Il problema di questi metodi è che possono subire attacchi di brute force anche offline, o attacchi reply, essendo crittograficamente piuttosto semplici.
- Si preferisce allora instaurare prima un tunnel TLS, e dentro al tunnel far passare le autenticazioni baste su User/Passwd.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Tunneled EAP

- EAP-TLS richiede espressamente che entrambe le parti si autentichino con dei certificati digitali, il che non è facilmente implementabile (poco *user friendly*).
- Esistono altri metodi per poter autenticare un utente su un database, di cui il più semplice è la coppia User/Passwd.
  - MD5
  - MSCHAP
  - LEAP
  - ...
- Il problema di questi metodi è che possono subire attacchi di brute force anche offline, o attacchi reply, essendo crittograficamente piuttosto semplici.
- Si preferisce allora instaurare prima un tunnel TLS, e dentro al tunnel far passare le autenticazioni baste su User/Passwd.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Tunneled EAP

- EAP-TLS richiede espressamente che entrambe le parti si autentichino con dei certificati digitali, il che non è facilmente implementabile (poco *user friendly*).
- Esistono altri metodi per poter autenticare un utente su un database, di cui il più semplice è la coppia User/Passwd.
  - MD5
  - MSCHAP
  - LEAP
  - ...
- Il problema di questi metodi è che possono subire attacchi di brute force anche offline, o attacchi reply, essendo crittograficamente piuttosto semplici.
- Si preferisce allora instaurare prima un tunnel TLS, e dentro al tunnel far passare le autenticazioni baste su User/Passwd.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Tunneled EAP

- EAP-TLS richiede espressamente che entrambe le parti si autentichino con dei certificati digitali, il che non è facilmente implementabile (poco *user friendly*).
- Esistono altri metodi per poter autenticare un utente su un database, di cui il più semplice è la coppia User/Passwd.
  - MD5
  - MSCHAP
  - LEAP
  - ...
- Il problema di questi metodi è che possono subire attacchi di brute force anche offline, o attacchi reply, essendo crittograficamente piuttosto semplici.
- Si preferisce allora instaurare prima un tunnel TLS, e dentro al tunnel far passare le autenticazioni baste su User/Passwd.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Tunneled EAP

- EAP-TLS richiede espressamente che entrambe le parti si autentichino con dei certificati digitali, il che non è facilmente implementabile (poco *user friendly*).
- Esistono altri metodi per poter autenticare un utente su un database, di cui il più semplice è la coppia User/Passwd.
  - MD5
  - MSCHAP
  - LEAP
  - ...
- Il problema di questi metodi è che possono subire attacchi di brute force anche offline, o attacchi reply, essendo crittograficamente piuttosto semplici.
- Si preferisce allora instaurare prima un tunnel TLS, e dentro al tunnel far passare le autenticazioni baste su User/Passwd.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

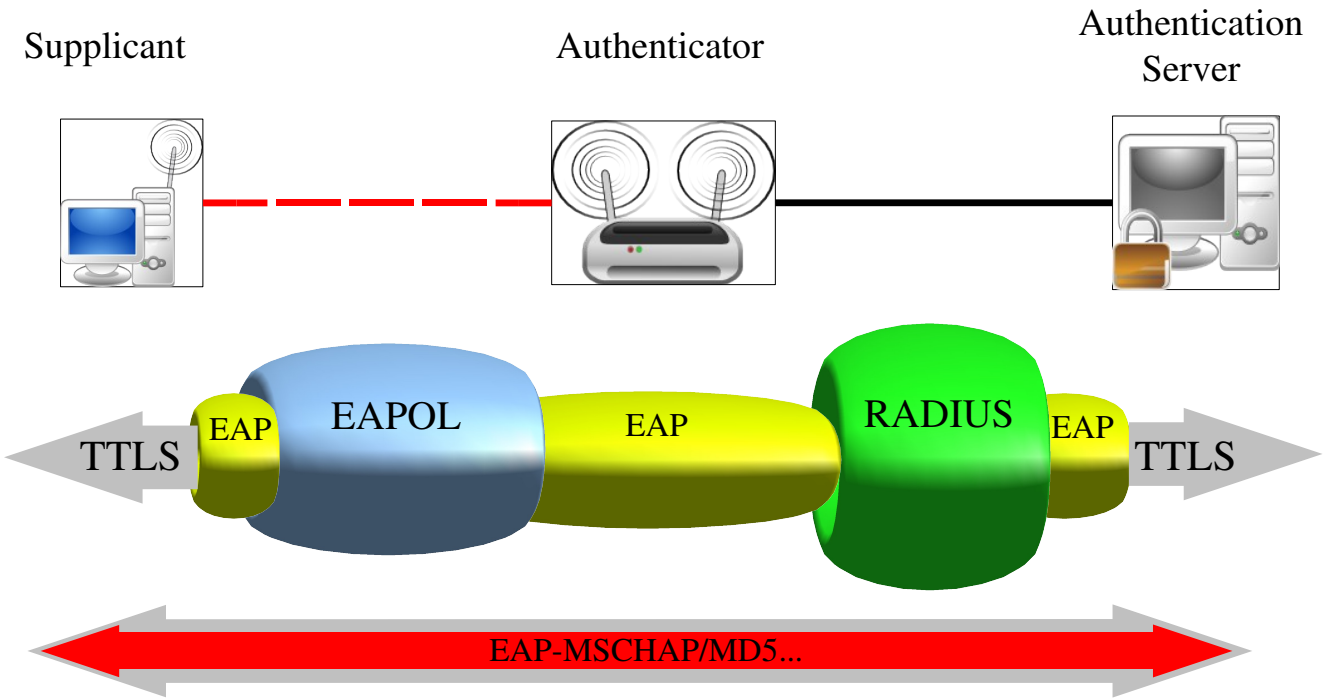
Tunneled EAP

- EAP-TLS richiede espressamente che entrambe le parti si autentichino con dei certificati digitali, il che non è facilmente implementabile (poco *user friendly*).
- Esistono altri metodi per poter autenticare un utente su un database, di cui il più semplice è la coppia User/Passwd.
  - MD5
  - MSCHAP
  - LEAP
  - ...
- Il problema di questi metodi è che possono subire attacchi di brute force anche offline, o attacchi reply, essendo crittograficamente piuttosto semplici.
- Si preferisce allora instaurare prima un tunnel TLS, e dentro al tunnel far passare le autenticazioni baste su User/Passwd.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

EAP-TTLS



Principi di crittografia:
- Cifratura a chiave simmetrica
- Cifratura a chiave pubblica/privata
- Funzioni hash
- Certificati

Il protocollo 802.11i
- 802.1X e 802.11i
- Protocolli coinvolti
- Metodi EAP
- Protocolli di tunnel
- RADIUS vulnerability

WPA-PSK

Varianti:

- PEAP è la versione Microsoft di TTLS, funziona sostanzialmente nello stesso modo.
- LEAP è la versione Cisco di TTLS

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Varianti:

- PEAP è la versione Microsoft di TTLS, funziona sostanzialmente nello stesso modo.
- LEAP è la versione Cisco di TTLS

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS

- RADIUS utilizza una chiave simmetrica per autenticare le richieste che l'*authenticator* fa all'*authentication server*.
- Ogni volta che l'*authenticator* inizia una sessione con l'*authentication server* invia un pacchetto di Access-Request. Nel pacchetto vengono specificate:
  - Username del *supplicant*.
  - Random Number.
- L'*authentication server* risponde con un messaggio di Accept/Reject/Challenge. In ogni caso aggiunge un campo di autenticazione:
- Se lo shared secret è una stringa prevedibile si può fare un attacco bruteforce offline.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS

- RADIUS utilizza una chiave simmetrica per autenticare le richieste che l'*authenticator* fa all'*authentication server*.
- Ogni volta che l'*authenticator* inizia una sessione con l'*authentication server* invia un pacchetto di Access-Request. Nel pacchetto vengono specificate:
  - Username del *supplicant*.
  - Random Number.
- L'*authentication server* risponde con un messaggio di Accept/Reject/Challenge. In ogni caso aggiunge un campo di autenticazione:
- Se lo shared secret è una stringa prevedibile si può fare un attacco bruteforce offline.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS

- RADIUS utilizza una chiave simmetrica per autenticare le richieste che l'*authenticator* fa all'*authentication server*.
- Ogni volta che l'*authenticator* inizia una sessione con l'*authentication server* invia un pacchetto di Access-Request. Nel pacchetto vengono specificate:
  - Username del *supplicant*.
  - Random Number.
- L'*authentication server* risponde con un messaggio di Accept/Reject/Challenge. In ogni caso aggiunge un campo di autenticazione:

  Authenticator = MD5(Code + Identifier + Length + RequestAuth + Attributes + Shared Secret)
- Se lo shared secret è una stringa prevedibile si può fare un attacco bruteforce offline.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS

- RADIUS utilizza una chiave simmetrica per autenticare le richieste che l'*authenticator* fa all'*authentication server*.
- Ogni volta che l'*authenticator* inizia una sessione con l'*authentication server* invia un pacchetto di Access-Request. Nel pacchetto vengono specificate:
  - Username del *supplicant*.
  - Random Number.
- L'*authentication server* risponde con un messaggio di Accept/Reject/Challenge. In ogni caso aggiunge un campo di autenticazione:
  - Auth = MD5(Code + Identifier + Length + Random Number + Attributes + Shared Secret)
- Se lo shared secret è una stringa prevedibile si può fare un attacco bruteforce offline.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS

- RADIUS utilizza una chiave simmetrica per autenticare le richieste che l'*authenticator* fa all'*authentication server*.
- Ogni volta che l'*authenticator* inizia una sessione con l'*authentication server* invia un pacchetto di Access-Request. Nel pacchetto vengono specificate:
  - Username del *supplicant*.
  - Random Number.
- L'*authentication server* risponde con un messaggio di Accept/Reject/Challenge. In ogni caso aggiunge un campo di autenticazione:
  - Auth = MD5(Code + Identifier + Length + Random Number + Attributes + Shared Secret)
- Se lo shared secret è una stringa prevedibile si può fare un attacco bruteforce offline.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS

- RADIUS utilizza una chiave simmetrica per autenticare le richieste che l'*authenticator* fa all'*authentication server*.
- Ogni volta che l'*authenticator* inizia una sessione con l'*authentication server* invia un pacchetto di Access-Request. Nel pacchetto vengono specificate:
  - Username del *supplicant*.
  - Random Number.
- L'*authentication server* risponde con un messaggio di Accept/Reject/Challenge. In ogni caso aggiunge un campo di autenticazione:
  - Auth = MD5(Code + Identifier + Length + Random Number + Attributes + Shared Secret)
- Se lo shared secret è una stringa prevedibile si può fare un attacco bruteforce offline.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS

- RADIUS utilizza una chiave simmetrica per autenticare le richieste che l'*authenticator* fa all'*authentication server*.
- Ogni volta che l'*authenticator* inizia una sessione con l'*authentication server* invia un pacchetto di Access-Request. Nel pacchetto vengono specificate:
  - Username del *supplicant*.
  - Random Number.
- L'*authentication server* risponde con un messaggio di Accept/Reject/Challenge. In ogni caso aggiunge un campo di autenticazione:
  - Auth = MD5(Code + Identifier + Length + Random Number + Attributes + Shared Secret)
- Se lo shared secret è una stringa prevedibile si può fare un attacco bruteforce offline.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS brute force

- L'attaccante raccoglie i pacchetti dell'autenticazione RADIUS.
- In locale genera ripetutamente gli *hash* utilizzando:
  - Un dizionario di parole chiave comuni (vocabolario, wordlist)
  - Un attacco esaustivo su tutte le parole generabile a partire da un set ristretto di caratteri ASCII.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS brute force

- L'attaccante raccoglie i pacchetti dell'autenticazione RADIUS.
- In locale genera ripetutamente gli *hash* utilizzando:
  - Un dizionario di parole chiave comuni (vocabolario, wordlist)
  - Un attacco esaustivo su tutte le parole generabile a partire da un set ristretto di caratteri ASCII.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS brute force

- L'attaccante raccoglie i pacchetti dell'autenticazione RADIUS.
- In locale genera ripetutamente gli *hash* utilizzando:
  - Un dizionario di parole chiave comuni (vocabolario, wordlist)
  - Un attacco esaustivo su tutte le parole generabile a partire da un set ristretto di caratteri ASCII.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS brute force

- L'attaccante raccoglie i pacchetti dell'autenticazione RADIUS.
- In locale genera ripetutamente gli *hash* utilizzando:
  - Un dizionario di parole chiave comuni (vocabolario, wordlist)
  - Un attacco esaustivo su tutte le parole generabile a partire da un set ristretto di caratteri ASCII.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS brute force

- Non è detto che l'attaccante possa ottenere i pacchetti RADIUS, che passano nel canale *authenticator* → *authentication server*. É possibile, per esempio se si utilizza il WDS.
- Mettere lo shared secret in fondo all'hash rende l'attacco computazionalmente più facile:
  - Con un pentium 4 si può realizzare un attacco esaustivo verso password alfanumeriche fino a 8 caratteri.
  - Con hardware dedicato ($$) si possono rompere password di 8 caratteri composte da tutti i 128 simboli ASCII in circa 34 giorni, in 90 minuti per sole passwd alfanumeriche.
- Soluzione: RADIUS over VPN.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS brute force

- Non è detto che l'attaccante possa ottenere i pacchetti RADIUS, che passano nel canale *authenticator* → *authentication server*. É possibile, per esempio se si utilizza il WDS.
- Mettere lo shared secret in fondo all'hash rende l'attacco computazionalmente più facile:
  - Con un pentium 4 si può realizzare un attacco esaustivo verso password alfanumeriche fino a 8 caratteri.
  - Con hardware dedicato ($$) si possono rompere password di 8 caratteri composte da tutti i 128 simboli ASCII in circa 34 giorni, in 90 minuti per sole passwd alfanumeriche.
- Soluzione: RADIUS over VPN.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS brute force

- Non è detto che l'attaccante possa ottenere i pacchetti RADIUS, che passano nel canale *authenticator* → *authentication server*. É possibile, per esempio se si utilizza il WDS.
- Mettere lo shared secret in fondo all'hash rende l'attacco computazionalmente più facile:
  - Con un pentium 4 si può realizzare un attacco esaustivo verso password alfanumeriche fino a 8 caratteri.
  - Con hardware dedicato ($$) si possono rompere password di 8 caratteri composte da tutti i 128 simboli ASCII in circa 34 giorni, in 90 minuti per sole passwd alfanumeriche.
- Soluzione: RADIUS over VPN.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS brute force

- Non è detto che l'attaccante possa ottenere i pacchetti RADIUS, che passano nel canale *authenticator* → *authentication server*. É possibile, per esempio se si utilizza il WDS.
- Mettere lo shared secret in fondo all'hash rende l'attacco computazionalmente più facile:
  - Con un pentium 4 si può realizzare un attacco esaustivo verso password alfanumeriche fino a 8 caratteri.
  - Con hardware dedicato ($$) si possono rompere password di 8 caratteri composte da tutti i 128 simboli ASCII in circa 34 giorni, in 90 minuti per sole passwd alfanumeriche.
- Soluzione: RADIUS over VPN.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

RADIUS brute force

- Non è detto che l'attaccante possa ottenere i pacchetti RADIUS, che passano nel canale *authenticator* $\rightarrow$ *authentication server*. É possibile, per esempio se si utilizza il WDS.
- Mettere lo shared secret in fondo all'hash rende l'attacco computazionalmente più facile:
  - Con un pentium 4 si può realizzare un attacco esaustivo verso password alfanumeriche fino a 8 caratteri.
  - Con hardware dedicato ($$) si possono rompere password di 8 caratteri composte da tutti i 128 simboli ASCII in circa 34 giorni, in 90 minuti per sole passwd alfanumeriche.
- Soluzione: RADIUS over VPN.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA Home

- Se non si vuole utilizzare un *authentication server* si possono impostare le chiavi PMK direttamente nel *supplicant* e nell'*authenticator*. Si parla di PSK Pre-Shared Key.
- Tutto funziona nello stesso modo, ma si salta la parte di autenticazione EAP e si prosegue dagli handshake.
- Le PSK possono essere configurate in una lista, associate ai MAC address delle schede di rete dei client.
- Una PSK è costituita da 256 bit e può essere specificata come:

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA Home

- Se non si vuole utilizzare un *authentication server* si possono impostare le chiavi PMK direttamente nel *supplicant* e nell'*authenticator*. Si parla di PSK Pre-Shared Key.
- Tutto funziona nello stesso modo, ma si salta la parte di autenticazione EAP e si prosegue dagli handshake.
- Le PSK possono essere configurate in una lista, associate ai MAC address delle schede di rete dei client.
- Una PSK è costituita da 256 bit e può essere specificata come:
  - 64 cifre esadecimali (0-9, A-F)
  - 8-63 caratteri ASCII, che vengono trasformati in PSK con PBKDF2

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA Home

- Se non si vuole utilizzare un *authentication server* si possono impostare le chiavi PMK direttamente nel *supplicant* e nell'*authenticator*. Si parla di PSK Pre-Shared Key.
- Tutto funziona nello stesso modo, ma si salta la parte di autenticazione EAP e si prosegue dagli handshake.
- Le PSK possono essere configurate in una lista, associate ai MAC address delle schede di rete dei client.
- Una PSK è costituita da 256 bit e può essere specificata come:
  - Una stringa in esadecimale: 0xa39f16ed6...
  - Una password che viene trasformata in 256 bit di chiave PSK.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA Home

- Se non si vuole utilizzare un *authentication server* si possono impostare le chiavi PMK direttamente nel *supplicant* e nell'*authenticator*. Si parla di PSK Pre-Shared Key.
- Tutto funziona nello stesso modo, ma si salta la parte di autenticazione EAP e si prosegue dagli handshake.
- Le PSK possono essere configurate in una lista, associate ai MAC address delle schede di rete dei client.
- Una PSK è costituita da 256 bit e può essere specificata come:
  - Una stringa in esadecimale: 0xa39f16ed6. . .
  - Una password che viene trasformata in 256 bit di chiave PSK.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA Home

- Se non si vuole utilizzare un *authentication server* si possono impostare le chiavi PMK direttamente nel *supplicant* e nell'*authenticator*. Si parla di PSK Pre-Shared Key.
- Tutto funziona nello stesso modo, ma si salta la parte di autenticazione EAP e si prosegue dagli handshake.
- Le PSK possono essere configurate in una lista, associate ai MAC address delle schede di rete dei client.
- Una PSK è costituita da 256 bit e può essere specificata come:
  - Una stringa in esadecimale: 0xa39f16ed6. . .
  - Una password che viene trasformata in 256 bit di chiave PSK.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA Home

- Se non si vuole utilizzare un *authentication server* si possono impostare le chiavi PMK direttamente nel *supplicant* e nell'*authenticator*. Si parla di PSK Pre-Shared Key.
- Tutto funziona nello stesso modo, ma si salta la parte di autenticazione EAP e si prosegue dagli handshake.
- Le PSK possono essere configurate in una lista, associate ai MAC address delle schede di rete dei client.
- Una PSK è costituita da 256 bit e può essere specificata come:
  - Una stringa in esadecimale: 0xa39f16ed6. . .
  - Una password che viene trasformata in 256 bit di chiave PSK.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

- Lo standard specifica una modalità perlomeno *consigliata* di traduzione dalla PSK al segreto:
  - PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)
- Notare che la PSK cambia anche se si cambia l'ESSID della rete.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

- Lo standard specifica una modalità perlomeno *consigliata* di traduzione dalla PSK al segreto:
  - PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)
- Notare che la PSK cambia anche se si cambia l'ESSID della rete.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

- Lo standard specifica una modalità perlomeno *consigliata* di traduzione dalla PSK al segreto:
  - PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)
- Notare che la PSK cambia anche se si cambia l'ESSID della rete.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

Lo standard consiglia:

- *A pass-phrase typically has about 2.5 bits of security per character, so the pass-phrase mapping converts an n octet password into a key with about 2.5n + 12 bits of security. Hence, it provides a relatively low level of security, with keys generated from short passwords subject to dictionary attack. Use of the key hash is recommended only where it is impractical to make use of a stronger form of user authentication. A key generated from a pass-phrase of less than about 20 characters is unlikely to deter attacks.*

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

Brute force sulla password:

- La PSK viene utilizzata nel 4-way handshake per generare la PTK.
- Raccogliendo i pacchetti di un 4-way handshake si può effettuare un attacco off-line utilizzando un dizionario di password.
- Per forzare un 4-way handshake si può inviare un pacchetto di deautenticazione e forzare la ripetizione di tutta la procedura.
- Per essere ragionevolmente sicuri di non poter essere vittima di attacchi di brute force bisogna:
- Entrambe le soluzioni sono puttosto scomode.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

Brute force sulla password:

- La PSK viene utilizzata nel 4-way handshake per generare la PTK.
- Raccogliendo i pacchetti di un 4-way handshake si può effettuare un attacco off-line utilizzando un dizionario di password.
- Per forzare un 4-way handshake si può inviare un pacchetto di deautenticazione e forzare la ripetizione di tutta la procedura.
- Per essere ragionevolmente sicuri di non poter essere vittima di attacchi di brute force bisogna:
  - o usare una password di 20 caratteri
  - o usare una PSK di 64 caratteri esadecimali
- Entrambe le soluzioni sono puttosto scomode.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

Brute force sulla password:

- La PSK viene utilizzata nel 4-way handshake per generare la PTK.
- Raccogliendo i pacchetti di un 4-way handshake si può effettuare un attacco off-line utilizzando un dizionario di password.
- Per forzare un 4-way handshake si può inviare un pacchetto di deautenticazione e forzare la ripetizione di tutta la procedura.
- Per essere ragionevolmente sicuri di non poter essere vittima di attacchi di brute force bisogna:
  - scegliere pasphrase di più di 20 caratteri.
  - utilizzare PSK in esadecimale.
- Entrambe le soluzioni sono puttosto scomode.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

Brute force sulla password:

- La PSK viene utilizzata nel 4-way handshake per generare la PTK.
- Raccogliendo i pacchetti di un 4-way handshake si può effettuare un attacco off-line utilizzando un dizionario di password.
- Per forzare un 4-way handshake si può inviare un pacchetto di deautenticazione e forzare la ripetizione di tutta la procedura.
- Per essere ragionevolmente sicuri di non poter essere vittima di attacchi di brute force bisogna:
  - scegliere pasphrase di più di 20 caratteri.
  - utilizzare PSK in esadecimale.
- Entrambe le soluzioni sono puttosto scomode.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

Brute force sulla password:

- La PSK viene utilizzata nel 4-way handshake per generare la PTK.
- Raccogliendo i pacchetti di un 4-way handshake si può effettuare un attacco off-line utilizzando un dizionario di password.
- Per forzare un 4-way handshake si può inviare un pacchetto di deautenticazione e forzare la ripetizione di tutta la procedura.
- Per essere ragionevolmente sicuri di non poter essere vittima di attacchi di brute force bisogna:
  - scegliere pasphrase di più di 20 caratteri.
  - utilizzare PSK in esadecimale.
- Entrambe le soluzioni sono puttosto scomode.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

Brute force sulla password:

- La PSK viene utilizzata nel 4-way handshake per generare la PTK.
- Raccogliendo i pacchetti di un 4-way handshake si può effettuare un attacco off-line utilizzando un dizionario di password.
- Per forzare un 4-way handshake si può inviare un pacchetto di deautenticazione e forzare la ripetizione di tutta la procedura.
- Per essere ragionevolmente sicuri di non poter essere vittima di attacchi di brute force bisogna:
  - scegliere pasphrase di più di 20 caratteri.
  - utilizzare PSK in esadecimale.
- Entrambe le soluzioni sono puttosto scomode.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

WPA-PSK

Brute force sulla password:

- La PSK viene utilizzata nel 4-way handshake per generare la PTK.
- Raccogliendo i pacchetti di un 4-way handshake si può effettuare un attacco off-line utilizzando un dizionario di password.
- Per forzare un 4-way handshake si può inviare un pacchetto di deautenticazione e forzare la ripetizione di tutta la procedura.
- Per essere ragionevolmente sicuri di non poter essere vittima di attacchi di brute force bisogna:
  - scegliere pasphrase di più di 20 caratteri.
  - utilizzare PSK in esadecimale.
- Entrambe le soluzioni sono puttosto scomode.

Leonardo Maccari,
maccari@lart.det.unifi.it

Principi di crittografia:
Cifratura a chiave simmetrica
Cifratura a chiave pubblica/privata
Funzioni hash
Certificati
Il protocollo 802.11i
802.1X e 802.11i
Protocolli coinvolti
Metodi EAP
Protocolli di tunnel
RADIUS vulnerability
WPA-PSK

Leonardo Maccari,
maccari@lart.det.unifi.it

Riferimenti

- Tutorial su 802.11i
- 4-way handshake, dalla PMK alla PTK
- Un articolo introduttivo su 802.11i
- Elenco di link sulla sicurezza di 802.11
- Altre slides su 802.11i

Leonardo Maccari,
maccari@lart.det.unifi.it

Riferimenti

- Tutorial su 802.11i
- 4-way handshake, dalla PMK alla PTK
- Un articolo introduttivo su 802.11i
- Elenco di link sulla sicurezza di 802.11
- Altre slides su 802.11i

Leonardo Maccari,
maccari@lart.det.unifi.it

Riferimenti

- Tutorial su 802.11i
- 4-way handshake, dalla PMK alla PTK
- Un articolo introduttivo su 802.11i
- Elenco di link sulla sicurezza di 802.11
- Altre slides su 802.11i

Leonardo Maccari,
maccari@lart.det.unifi.it

Riferimenti

- Tutorial su 802.11i
- 4-way handshake, dalla PMK alla PTK
- Un articolo introduttivo su 802.11i
- Elenco di link sulla sicurezza di 802.11
- Altre slides su 802.11i

Leonardo Maccari,
maccari@lart.det.unifi.it

Riferimenti

- Tutorial su 802.11i
- 4-way handshake, dalla PMK alla PTK
- Un articolo introduttivo su 802.11i
- Elenco di link sulla sicurezza di 802.11
- Altre slides su 802.11i