Contents

1 Introduzione-warm up example

Il problema spesso è che una buona crittografia è applicata male alla risoluzione di un problema.esempio: paper che discute di una tecnica di sicurezza ed in cui viene matematicamente provata la sicurezza.
Basata sul meccanismo del One Time Pad: ho il mio plain text e voglio criptarlo in modo che non si capisca cosa ci sia scritto. Genero una sequenza random di bit, di lunghezza pari alla lunghezza del testo. Una volta ottenuta la chiave, computo lo XOR fra la chiave ed il plaintext ed ottengo il mio ciphertext.

Il seguente meccanismo è il migliore possibile per fare enrcyption.
Per decriptare applico il procedimento inverso, facendo sempre l'XOR, infatti: $b \oplus 1 = \bar{b} \oplus 1 = b$.
Devo però fare delle assunzioni:

1. Per ogni nuovo messaggi, devo usare una diversa chiave. Questo perché, se ripetessi la chiave avrei il peggior meccanismo di enrcyption: se ho due messaggi M_1 ed M_2, ed ottengo $C_1 = M_1 \oplus K$ e $C_2 = M_2 \oplus K$, ora facendo $C_1 \oplus C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K) = M_1 \oplus M_2$ (in quanto $K \oplus K$ si elide).Conoscendo uno dei due messaggi posso ricavare l'altro.

2. La chiave deve essere lunga quanto il plaintext

3. La chiave deve essere veramente random, e non pseudorandom.

L'algoritmo introdotto sopra è chiamato Vernam Cipher, ed è il miglior meccanismo di enrcyption possibile.
Il problema nel metterlo in pratica è che la chiave deve essere nota sia a chi produce il messaggio, sia a chi lo riceve, quindi va trasmessa su un canale sicuro. Se le dimensioni della chiave cominciano a diventare considerevoli, ad esempio per 2GB di plaintext devo avere 2GB di chiave, il costo d'invio al receiver diventa oneroso.
Quando si parla di sicurezza, non bisogna chiedersi come rendere il sistema sicuro, ma da cosa devo difendermi, di cosa è capace l'attaccante.
OTP protegge la confidenzialità, ma non garantisce l'integrità.
Le 3 proprietà che posso/voglio garantire sono:

- Confidenzialità: proteggo i dati da persone esterne,che non possono leggere il contenuto senza una chiave

- Integrità: voglio che i miei dati rimangano inalterati

- Aviability: mi proteggo, ad esempio da DDoS

Nel caso di OTP, l'integrità non è garantita: se un avversario prende il mio messaggio e lo cambia,ad esempio flippando alcuni byte (Man in the middle attack) non riesco a rendermene conto; l'avversario ha agito sul testo cifrato, senza interessarsi del,contenuto.

2 Encryption

Servizio di sicurezza che vuole proteggere la confidenzialità dei dati, non protegge però l'integrità. Si parte dal plaintext $\longrightarrow$ encryption $\longrightarrow$ cipher text $\longrightarrow$ invio $\longrightarrow$ decryption $\longrightarrow$ plaintext.
Servono delle chiavi per potere de/criptare, per ora mi concentro sul meccanismo della symmetric key: sia sender che receiver usano la stessa chiave. Il cipher sarà il mio algoritmo per criptare e decriptare:
C = ENC(K,P) D = DEC(K,C).

2.1 Esempi storici di cipher

Un primo esempio può essere quello di sostituire le lettere del plaintext con altre lettere, in maniera reversibile ovvero se a $\longrightarrow$ b, non posso avere c $\longrightarrow$ b.
Posso decriptare in maniera veloce? Vedo la frequenza delle lettere di una lingua, ad esempio l'italiano, e saprò quali lettere compaiono più spesso in un plaintext, inoltre posso avere delle parole con delle ripetizioni interne.
Procedo per tentativi, nel momento in cui deduco una lettera, la associo ad una più o meno probabile.
Posso inoltre ricavare la chiave usata per criptare.
Il metodo è storico (me pare addirittura lo usavano i romani sotto Cesare), quindi fortemente sconsigliato.

2.2 RFID mutual authentication

Vernam cipher è il miglior meccanismo, ma ha delle forti implicazioni. Considero una situazione reale:
ho un TAG, ed un reader presso cui devo autenticarmi. Il TAG ha lo scopo di provare al reader che l'utente è davvero reale, ma anche il reader dovrebbe dimostrare di essere sicuro; voglio quindi che l'autenticazione sia mutua.
Ho un segreto S, scritto ad esempio in una mia carta d'autenticazione e quando mi approccio al reader mi devo identificare. Ho due probelmi:

- La trasmissione avviene su un canale wireless, se poi la trasmissione è in chiaro un attacker può captare e rubare S
- Se il reader è falso, ora conosce il mio segreto S

Vorrei poter autenticarmi senza mostrare il segreto S esplicitamente, uso uno schema:
il TAG ha un segreto S,statico, ed una chiave temporanea k. Invece di trasmettere S, invio k $\oplus$ S al reader, che avrà un database in cui ha il segreto salvato e la chiave k. Il reader riesegue quindi lo XOR e vede se il risultato coincide con quello che gli ho inviato io. La prossima chiave sarà generata dal reader a partire da k, quindi con un meccanismo pseudorandom. Provo ad usare un former analyzer, che mi garantisce che il sistema è sicuro (software che prova a crackare il meccanismo di encryption). Sono realmente sicuro?
Ho l'operazione k $\oplus$ S, k è pseudorandom e posso avere due situazioni:

1. S è la chiave: sto violando la proprietà 1, in quanto riuso S più volte per messaggi diversi
2. k è la chiave: se faccio $(S \oplus k_i) \oplus (S \oplus k_{i+1}) = k_i \oplus k_{i+1}$. Non ho violato il sistema, ma ho la combinazione delle due chiavi, che sono pseudorandom: ho x $\oplus$ f(x) (PNRG(x)), x dipende da f(x), quindi posso fare un ciclo fino al valore massimo, controllo se $z_i = x_i \oplus \text{PNRG}(x_i)$, alla fine ricaverò k_i.

Il meccanismo non può essere risolto in alcun modo, le assunzioni erano errate, quindi:

- Former analyzers non sono una certezza, bisogna comunque verificare che l'assunzione è corretta
- Random e pseudorandom sono completamente diversi

2.3 Sicurezza di un cipher

Un cipher è sicuro quando:

- protegge la confidenzialità
- nasconde i messaggi
- non può essere violato

Ma questa definizione è una supercazzola (serio, così ha detto il prof a lezione e così scrivo io negli appunti), e anche altre definizioni sono brutte e sbagliate. Un cipher può essere sicuro per un determinato attacco che vuole svelare il contenuto, ma non sicuro per un altro che vuole vedere solo parte delle coppie plaintext-ciphertext.
Ad esempio un chosen plaintext attack permette di vedere sia plaintext che ciphertext, voglio essere robusto quantomeno a questo tipo di attacco.
Definizione di semantically secure o IND-CPA, ovvero Indistinguishability Under Chosen Plaintext Attack.
esempio: ho due messaggi, M_0 ed M_1, suppongo di poter criptare solo uno dei due.
Permetto all attacker di mandarmi i due messaggi ed io scelgo a caso quale dei due criptare con un coinflip. Mando indietro il messaggio cifrato all'attaccante: in condizioni normali l'attacante può facilmente decriptare il messaggio, se usassi un cipher non semantically secure, ma ora entra in gioco IND-CPA $\Rightarrow$ l'attaccante ha una probabilità del 50% di ottenere il messaggio corretto, ovvero deve scegliere a caso fra i due.I sistema sarà semantically secure se l'avversario non può risolvere questa situazione: ha a disposizione un oracolo, che gli fornisce l'encryption dei due messagi, quindi se uso un meccanismo di encryption sostitutivo (vedi esempio de Giulio Cesare) $\Rightarrow$ GAME OVER. Ora uso una chiave random (esempio Vernam Cipher): allo stesso plaintext corrispondono ciphertext diversi, quindi l'oracolo non può fornire il risultato esatto all'attaccante. L'unico modo che ha per vincere è di tirare ad indovinare, quindi con un coinflip.
L'encryption deve essere random, perché se una sotto stringa si ripete non deve corrispondere allo stesso ciphertext. Lo XOR è random:
bit segreto $\oplus$ bit random
bit segreto: 0 = p, 1 = 1-p
bit random: $0 = \frac{1}{2}$, $1 = \frac{1}{2}$
Avrò quindi:
Quindi il Vernam ciper è perfettamente random: l'avversario vede solo il cipher text, quindi può indovinare 0 o 1 con probabilità: $\frac{p}{2} + \frac{(1-p)}{2} = \frac{1}{2}$. Vernam cipher è però teorico e nella pratica si usano altri cipher, divisi in categorie:

bit segreto	bit random	XOR	probabilità
0	0	0	$\frac{p}{2}$
0	1	1	$\frac{p}{2}$
1	0	1	$\frac{(1-p)}{2}$
1	1	0	$\frac{(1-p)}{2}$

- stream cipher: un mimic di Vernam cipher, usa un algoritmo pseudorandom usando lo XOR, il più famoso era RC4, oggi si usano Salsa20 e ChaCha20.
- Block cipher: il più usato è AES, usano una tecnica diversa
- Block cipher in stream mode: AES-CTR, il block cipher genera una chiave pseudorandom e poi usa uno stream cipher.

2.4 Stream cipher

L'obbiettivo è quello di approssimare One Time Pad: invece di usare una chiave random, uso una chiave di 128 bit come seed per uno stream di bit pseudorandom, che sarà il keystream.
Usa poi lo XOR, la chiave è più corta e viene incrementata con il keystream: l'algoritmo pseudorandom è progettato ad hoc, non è il classico pseudorandom. La differenza cruciale con OTP è che la chiave è generata a partire da una chiave k piccola, quindi posso trasmettere k al receiver facilmente. Ma se k è sempre la stessa ho un problema, ovvero encrypto sempre con la stessa key di base. Se una sottostringa si ripete, avrò ciphertext diverso (la periodicità del sistema pseudorandom deve essere molto lunga), ma per lo stesso messaggio ho lo stesso ciphertext, in quanto l'algoritmo pseudorandom deterministico. Vorrei comunicare la chiave una volta per tutte senza doverla cambiare (come avviene in Wi Fi access point), ho una chiave k piccola ed un keystream lungo, ma non sono IND-CPA.

2.4.1 Initialization vector

Ho un plaintext che voglio cifrare, mando un messaggio alla mia NIC in modo che lo encrypti con un algoritmo di tipo stream cipher. La NIC ha una chiave k a lungo termine e quando riceve il messaggio genera una quantità dinamica,che è l'initialization vector (IV); questa quantità può essere truly random. Il seed sarà generato giustapponendo la chiave k all'IV, che mi fornirà il keystream, ovviamente l'IV deve essere diverso per ogni messaggio. Come comunico all'altro end l'IV? Lo mando in chiaro con il messaggio, se lo strem cipher è buono non posso determinare il messaggio a partire dall'initialization vector. Ora il receiver può riprodurre il keystream: fa lo XOR e decripta il messaggio ricevuto; l'ipotesi fondamentale è che il PRNG sia buono.
Ho la prova di essere semantically secure se l'IV non si ripete.

2.4.2 Case study: WEP 802.11

Wired Equivalent Privacy, standardizzato nel 1997-1999 dagli stessi progettisti di Wi-Fi. Aveva 3 obbiettivi:

- confidenzialità: proteggere i pacchetti da qualcuno di esterno alla rete, uso dell'algoritmo stream cipher RC4 (poi scoperto vulnerabile, ma è n'altra storia).
- integrità: il pacchetto non doveva essere modificato lungo il tragitto.
- : autenticazione: voglio che qualcuno possa entrare nella rete solo tramite delle credenziali.

2.4.3 RC4

Algoritmo PRNG specifico, usato per generare il keystream. Oggi è considerato debole, ma comunque WEP avrebbe avuto gli stessi problemi anche se fosse stato buono.
ENC(KEY,MSG) = MSG $\oplus$ RC4(KEY,IV)
L'IV va generato per ogni frame e deve essere diverso per ognuno di essi, inoltre lo stream cipher deve essere sincronizzato in un canale che ha perdita. L'IV viene trasmesso in chiaro, se lo stream cipher è buono è buono non ho problemi. WEP è sicuro se l'IV non si ripete, altrimenti userei la stessa chiave e non avrei semantic security.
In Wi-Fi è "semplice" attaccare con Chosen Plaintext Attack o Known Plaintext Attack, anche se non conosco i messaggi ma li vedo in XOR posso ricavare qualcosa, l'IV è quindi cruciale e in WEP furono commessi due errori:

- La taglia era di 24 bit, molto piccola: circa 16.7 milioni di encryption diversi, se assumo 1500 byte di trama, con 7 Mbps di thoughput $\Rightarrow$ riciclo dopo appena 8 ore.
- L'implementazione fu lasciata libera $\Rightarrow$ COSA DA NON FARE MAI, MAI-IIII M A I (MAI PIÙÙÙÙÙÙÙÙÙÙ NON NOMINARE MIA MADRE CIT*), potrebbero metterci tutti 00..0 se non leggono la specifica.

Inoltre, conviene generare l'IV random o in maniera sequenziale? Se lo genero random, ho il 50% di probabilità di avere un duplicato dopo circa 4000 frame (birthday paradox).Meglio quindi sceglierli in serie, però sono suscettibile ad un attacco: se il router viene spento e riacceso, la sequenza riparte da 0. L'attacker può catturare i messaggi, rebootare di nuovo e fare un Chosen Plaintext Attack, ricreando la sequenza degli IV.
Il reboot dovrebbe prevedere un seed sempre diverso, ma qui il generatore è PRNG.
L'attacker può quindi creare un dizionario:
per ogni IV avrà il corrispondente keystream = RC4(IV,K), così da poter usare la coppia per attaccare (manda un contenuto noto ed una volta ricevuta la risposta ricava MSG $\oplus$ keystream $\oplus$ MSG ed ottiene il keystream).

Se RC4 è buono, non deve essere possibile ricavare una entry del dizionario avendo tutte le restanti. Un altro attacco può consistere nell'aspettare che l'IV si ripeta.

2.4.4 User authentication

Autenticazione: mostrare davvero chi sei. Non va confusa con l'identificazione, con cui fornisco nome cognome etc..., l'autenticazione è la prova che controllo la mia identità digitale.
Non è semplice definire l'autenticazione, molti siti difatti permettono di creare ad esempio mail che non mostrano il mio nome e cognome e quindi questo non mi identifica, ma voglio comunque che l'account sia usato da una sola persona.
Metodi di autenticazione:

- Metodo "base": una password, un pin, chiave segreta etc...
- device fisici: smart card, token digitali, hardware non clonabile.
- biometrics: impronta digitale, retina etc...
- behavioural authentication: registrazione vocale, hand writing etc...

In WEP non fu prevista l'autenticazione di ogni singolo utente. L'obiettivo era quello di riuscire ad autenticare un gruppo di persone che potessero entrare nella rete. L'idea: chi sta nella stessa rete può essere visto dagli altri, quindi usa los etsso meccanismo di enrcyption.
Il grant di accesso era dato solo a chi aveva una password comune, pre-distribuita.
Come provare l'autenticazione: non posso inviarla in chiaro (sono in Wi-Fi), quindi in WEP venne introdotto un meccanismo che prevedeva di effettuare delle operazioni sulla password; il risultato non doveva dare informazioni sulla password.
Meccanismo: conosco k, l'access point mi manda una challenge ed io gli fornisco un encryption della challenge e della password.Per ogni nuovo utente devo usare una challenge diversa, può seere una stringa in plaintext, in WEP era di 128 bit. Una volta ricevuta la risposta, l'AP decriptava e se il risultato era la k dava l'accesso.Tecnica symmetric key, buona? Sì, trovo in un libro scritto da gente top nel settore che mi descrive esattamente questa tecnica, se la challenge è random e senza ripetizioni sono al sicuro.
In WEP non è così,anzi l'autenticazione aiuta a violare la confidenzialità: come detto sopra, posso effettuare un Known Plaintext Attack per creare un dizionario IV — keystream = RC4(K,IV). Quello che vedo nel messaggio è chipertext = plaintext $\oplus$ keystream, devo conoscere il plaintext. WEP fornisce la possibilità di un KPA con l'autenticazione: CT $\oplus$ challenge = RC4(k, IV) = keystream. L'approccio è corretto, ma viene riusata la stessa chiave per cifrare la challenge ed i messaggi. La challenge inoltre è in plaintext $\longrightarrow$ nota $\longrightarrow$ Known Plaintext Attack.
Attacker si finge l'access point ed inviando challenge false costruisce il dizionario, una volta ottenuto il keystream (user mi manda challenge $\oplus$ keystream, io ho

la challenge, faccio $\oplus$ ed ottengo il keystream) posso usarlo per criptare la challenge successiva e ottenere l'accesso.
L'autenticazione era certificata come robusta, ma l'implementazione non lo era, inoltre l'IV era lasciato all'implementatore $\Rightarrow$ MAI FARLO.
Il fix fu di far scegliere sia la challenge che l'IV all'acces point, ma in ogni caso essendo l'IV corto si sarebbe ripetuto.

2.5 Integrità

Per l'integrità, l'idea fu quella di utilizzare CRC-32, il controllo a lvl2, come integrity check. Non è certo però che funzioni, ma l'attacker vedrà solo il ciphertext, quindi anche se il CRC-32 non è buono è protetto dall'encryption: assunzione errata. Confidenzialità non garantisce integrità. CRC-32 è lineare rispetto allo XOR: se faccio CRC32(A) e CRC(32) di B (con A e B due messaggi diversi) fare CRC32(A $\oplus$ B) = CRC32(A) $\oplus$ CRC32(B). Inoltre, lo XOR era proprio usato per l'encryption $\Rightarrow$ deadly. Ogni messaggio può subire modifiche o injection:
ho un plaintext M di, cui l'attacker vuole flippare 3 bit, ho CRC32(M), ed ho M $\oplus$ RC4(K,IV). Produco un messaggio δ che è uguale ad M, ma con i 3 bit che voglio flippare pari ad 1, computo CRC32(δ), prendo il precedente ciphertext e ne faccio lo XOR con il mio:
keystream $\oplus$ M $\oplus$ δ — keystream$_2$ $\oplus$ CRC(M $\oplus$ δ) (per linearità dello XOR).
Ho un nuovo messaggio valido (nelle ipotesi che δ sia pari ad M), quindi posso eseguire un Man in the middle attack.
Dopo WEP ci fu 802.11 in cui il protocollo è WPA (anche WPA2 con AES), venne inoltre eseguita una patch firmware a RC4:

- IV a 48 bit
- protezione dell'IV
- etc...

Morale: rivolgersi ad un esperto di crittografia.

3 Autenticazione in generale

Le password sono deboli, faccio una panoramica per capire se una password è hard o no. Autenticazione: provo che ho una password, che per ora ritengo analoga ad un segreto (in pratica: un segreto è una stringa random). Se ho 4 bit, ho 2^4 possibilità, quindi la probabilità di indovinare al primo tentativo è $\frac{1}{2^4}$.
Una password è una stringa con meno entropia: se ho una password di N bit, la probabilità di indovinare al primo tentativo è $>>$ di $\frac{1}{2^N}$.
Ho 4 problemi maggiori:

- password overload: gli utenti tendono a riutilizzare le password su più siti

- restricted charset: 1 byte = 8 bit, quindi 256 possibili combinazioni, ma da tastiera ne ho circa 100.
- low entropy: la password non è del tutto random, in quanto va comunque memorizzata.
- predictability: spesso le password sono associate alla vita reale

3.1 Password overload

Nel 2018, in USA, uno studio ha rivelato che ogni persona ha circa 130 account nel web: il 38% degli utenti riutilizza la stessa password su più siti. Se scopro una password di un account, posso usarla per accedere su altri siti ⇒ cross site break.
Il 21% degli utenti modifica la propria password, ma le modifiche sono predicibili, inoltre il 46.5% delle password si cracka con 100 tentativi.

3.2 Restricted charset

Se ho un segreto di 8 byte, quindi 64 bit, ogni byte ha 256 diverse possibilità, quindi la probabilità di guess al primo tentativo è $\frac{1}{256^8}$. È un numero elevato? Una macchina "ordinaria" può effettuare 66 milioni guess/secondo, quindi il tempo medio per crackare la password è di circa 4431 anni: $1.8\text{x}10^{19}$ tentativi totali, divido per il numero di guess/secondo e divido per 2 (per fare una media), converto in anni. Le password però non hanno 256 possibilità per ogni byte, inoltre alcune usano solo lettere lower case, o al più numeri. Anche se vengono introdotti numeri e lettere upper case/simboli, spesso vengono messi in posizioni predicibili (es: all'inizio, alla fine, nel mezzo).
Sto considerando un attack brute force offline, in quanto proteggere un web server sarebbe possibile, ade sempio bloccando l'accesso dopo il 3° attempt fallito.

3.3 Low entropy

Ci sono dei tool dell'information theory che misurano la randomness. Le password non sono quasi mai random. Come misuro la randomness: Shannon entropy: Entropia $\text{H(X)} = -\sum_i p_i log_2(p_i)$, considero $\text{p} > 0$, inoltre il segno meno serve perché essendo $\text{p} \leq 1$, il log mi da un valore negativo.
La quantità viene misurata in bit. esempio: un coinflip di una moneta equiprobabile ha $\text{H(X)} = -2 \cdot (\frac{1}{2} \cdot log_2(\frac{1}{2})) = 1$.
Per il dado ho $-6 \cdot (\frac{1}{6} \cdot log_2(\frac{1}{6})) = 2.58$. Per un random byte ho $-256 \cdot (\frac{1}{256} \cdot log_2(\frac{1}{256})) = log_2(256) = 8$, ma questo solo se i bit sono davvero random, altrimenti ho un valore minore di 8.
L'information value di x_i dipende da quanto x_i è inatteso: minore è la probabilità di un certo evento e più sono sorpreso, l'information content è quindi = $\frac{1}{p_i}$.

$log_2(\frac{1}{p_i})$ è una traslazione della probabilità in bit, ad esempio $\frac{1}{4}$ diventa 2 bit. L'information content è misurata quindi come $log_2(\frac{1}{p_i})$.
Definisco l'entropia come l'average dell'information content degli x_i: H(X) = E[IC(X)] = $\sum_i p_i IC_i = -\sum_i p_i log_2(p_i)$.
Entropia: misura quantitativa per vedere quanto un evento random è predicibile, se pari ad 8 ho un byte perfettamente random, se è 0 è deterministico. Se $N = 2^b$ possibili outcome allora b = $log_2(N)$, se l'entropia è pari a b, non posso predire. esempio: una moneta truccata con $\frac{1}{4}$ $\frac{3}{4}$ ho entropia pari a $0.81 < 1$, quindi è predicibile.
Conseguenze: quando trasmetto un bit, trasferisco una quantità minore di informazione, posso comprimere di (1-quantità)% un file.
esempio: genero 3 bit random, ho entropia pari a 3, ma se ci sono dipendenze? Ad esempio se solo il primo è un coinflip e gli altri due sono deterministici, ad esempio prendono il valore del primo ho entropia = 1. Non conta quindi la lunghezza della stringa, bensì la randomness.
Nel 1950, Shannon misurò l'entropia di un testo (in inglese), mostrando che il linguaggio naturale è molto predicibile:
le lettere che comparivano nel testo non erano equiprobabili, quindi l'information content della singola lettera non è 4.71 (ovvero non ho probabilità di $\frac{1}{26} \Rightarrow -log_2(\frac{1}{26})$. Nota la prima,l'entropia della seconda etc... sono in un certo modo predicibili, ogni lettera inglese ha nella migliore condizione 1.3 di information content e 0.6 nella peggiore. Ogni lettera ha un contributo $\simeq 2$, e quindi generando una password avrò un entropia di circa 2 bit invece di 8.
Se ho 10 lettere random:
tempo di crack se puramente random = $2^{4,7 \cdot 10} = 2^{47}$ attempts, mentre nel caso di password "umana" ho $2^{2 \cdot 10} = 2^{20}$ attempts; perdo un fattore $2^27 \simeq 134$ milioni, quindi molto meno robusta.

3.4 Predicibilità-Dictonary attack

In realtà, non serve nemmeno fare un brute force attack, ma si possono usare parole note. Faccio un dictionary attack: scelgo una serie di parole comuni in una lingua e faccio try su queste parole.
Se riesco a recuperare un set pubblico di password dal web quello brutto e cattivo costruisco il mio dizionario, che può anche essere mirato al singolo individuo (so nomi di familiari, date di nascita, gusti etc...).Gli attacchi funzionano sia online che offline, dove la forza dipende dalla potenza dell'hardware e dalla randomness della password.
Alcune statistiche:

- 25% delle password è del tipo 123456..., posso pensare anche ad un password sparying: prendo una passowrd e la provo su più account di diverse persone, in verticale (può essere molto efficace).
- 26% delle password sono di 6 byte, ne vanno usati almeno 16.

4 Autenticazione password-based vs autenticazione challenge-handshake

Dopo aver esaminato le password, vorrei un protocollo che mi permetta di usarle per autenticarmi. Ricordo che l'autenticazione è la prova di conoscere un segreto, senza dover per forza rivelarlo. Ho alcune alternative:

- PAP: mostro la password in chiaro
- CHAP: alcune informazioni leakate
- ZPK: nessuna informazione leakate (crypto forte), molto complessi e poco usati nella realtà

4.1 PAP

Il protocollo di autenticazione più semplice possibile: mando la password in chiaro, one way authentication. L'utente manda la sua password (insieme allo user id)ad un autenticatore, che fa un check nel DB in cui per vedere se ha una entry user id — password.
La password è pre-shared, ma la sto mandando in chiaro e se vengo intercettato è GAME OVER (se il canale permette eavesdropping, se è cablato sono leggermente più sl sicuro).
Inoltre non ho nessuna protezione da reply attack: se vengo intercettato, subito dopo l'attaccante può fingersi me, se non enrypto con un algoritmo semantically secure e se non ci sono limiti nel poter ripetere l'autenticazione; inoltre non permetto mutual authentication.
Il messaggio PAP è suddiviso in campi specifici a seconda del server a cui mi devo autenticare, se ad esempio ho server PPP: i campi sono espressi in ASCII ed ogni campo ha una semantica, me la studio, prendo il pacchetto e scopro tutte le info.

4.2 CHAP

L'authenticator mi manda una challenge, a cui rispondo con un messaggio contente il mio user id + hash(challenge,password,etc).Proof of knowledge: computazione di un segreto/password, mando una f(password) per dimostrare che la conosco. La funzione deve avere due proprietà:

- la computazione non deve rivelare il segreto, quindi non devo poter computare f^{-1}
- la funzione f non deve poter essere replicata da un attaccante.

L'authenticator mi manda una challenge ogni volta nuova, ovver una nonce. Lo user risponde con userID ed una funzione di challenge, key, etc...(parametri opzionali). La funzione deve rispettare le due proprietà, l'authenticator la ricalcola, dopo aver preso dal db la password corrispondente allo userID ricevuto; la

funzione deve quindi essere deterministica.
Se la challenge è fresh non sono suscettibile a reply attack, inoltre la password non è inviata in chiaro.
La funzione può essere una hash function crittografica.
In CHAP è l'autenticatore che controlla tutto il processo: potrebbe accadere che un'attacker potrebbe intercettare la mia sessione kickarmi, sostituendosi a me. Per prevenire ciò, in CHAP è possibile far si che l'authenticator rimandi la challenge periodicamente, per accertare l'autenticità dell'utente. Tutto ciò in PAP non è possibile, ma il grande svantaggio di CHAP è che le password devono essere salvate in chiaro nel db.

4.3 Hash function

Funzioni crittografiche di base. Prende qualcosa in input e la riduce in polvere in maniera che sia incomprensibile ed irreversibile. Se ho un messaggio di lunghezza X, Y=H(X) è detto digest ed ha una taglia fissa; H(X) dovrebbe essere abbastanza semplice da poter essere computata su ogni X.
Non è sempre detto che le funzioni hash sia crittografiche, alcuni esempi di funzioni non crittografiche:

- 4 bit parity vector checksum: prendob blocchi da 4 bit e metto un bit di parità sui blocchi. La size del digest (ottenuto giustapponendo i bit di parità) è sempre pari a 4, e la funzione non è invertibile, in quanto l'inversa non è unica
- modula checksum: spezzo in chunk di interi (valori $\in$ [0,..9]) il mio messaggio, li sommo e ne faccio il mod1000.
- call center control: devo autenticarmi con username e password, mi richiedono un pin ma non lo mando tutto, bensì solo specifiche cifre.

Ogni hash function, anche non crittografica, non è invertibile.
Un hash function crittografica prende il testo e lo comprime in un digest di dimensione fissa, ma ha un importante proprietà: anche piccoli cambiamenti producono digest completamente diversi.Deve cercare di approssimare al meglio la generazione di una stringa random.Nel caso di funzioni hash non crypto, un cambiamento minimo è abbastanza prevedibile.
Un attaccante non deve in alcun modo ricreare l'hash digest: nel caso di non-crypto hash, cambiando i bit posso ottenere un messaggio diverso che mi fornisce lo stesso digest $\Rightarrow$ collisione. L'attacker non dovrebbe essere in grado di poter ricreare o modificare il messaggio così da ottenere il digest originale. Devono valere 3 proprietà:

1. Perimage resistance (one-way property): dato y=digest, deve essere computazionalmente difficile trovare X tale che H(X)=Y. Proprietà più forte del non invertibile, la computazione non deve poter essere ricavabile, anche se ho infiniti emssaggi che generano lo stesso digest.

Corollario: per essere one-way la lunghezza del digest deve essere grande, non devo potervi fare brute force attacko crypto-analysis.

2. Weak collision resistance: dato X, è computazionalmente difficile trovare un X', che sia diverso da X, e tale per cui H(X) = H(X').esempio: sono un giudice di un tribunale, ho un hard disk su cui ci sono delle prove, lo do ad un esperto per analizzarlo. Come posso essere sicuro che le prove non siano inquinate? Computo l'hash dell'hard disk e lo metto ar pizzo (lo scrivo su un pizzino magari), così che se qualcuno inquina le prove gli do la sedia elettrica, perché vale questa proprietà e non può produrre modifiche tali per cui l'hash è lo stesso.

3. Strong collision resistance: ci sono funzioni che sono solide per la proprietà 1 ma non per la 2? Sì, ad esempio se considero Y= f(x) = $g^x modp$: g è dato, p è un numero primo molto grande. Se ad esempio so che 321475 = 3^x, riesco a ricavare x? Sì, ho che x = $\log_3 321475$, ma se aggiungo il *modp* non posso più farlo, non è facile computare l'inversa sotto determinate condizioni. Ma non rispetto la proprietà 2: se ho un X, mi basta sommare k·(p-1) per trovare lo stesso risultato; la funzione sembra difficile, ma non rispetta le proprietà.
Con la strong collision resistance voglio che sia impossibile trovare una qualunque coppia X_1, X_2 che collida.

4.4 Paradosso del compleanno e dimensione del digest

Voglio vedere come rispettare la strong collision resistance. Considero il birthday paradox: ho k=23 persone in una stanza, voglio associare a ciascuno un hash fatto sul loro giorno+mese di nascita. Probabilità che non ci siano collisioni tra uno dei k e gli altri k-1: $(\frac{364}{365})^{22} = 94.1\%$. Ma qual'è la probabilità che non ci siano collisioni tra tutti i k: $1 \cdot (1\text{-}\frac{1}{365}) \ldots\ldots \cdot (1\text{-}\frac{22}{365}) \simeq 49.3\%$. Quindi la probabilità di collidere è il complementare, ovvero 1-0.493 = 0.507 = 50.7%. esempio: ho n bit di digest, $N = 2^n$ diversi risultati. Considero k messaggi:
P(no collisioni) = 1-p = $\frac{\frac{N!}{(N-k+1)!}}{N^k} = \frac{N}{N} \cdot \frac{N-1}{N} \cdot \frac{N-2}{N} \ldots\ldots \cdot \frac{N-k+1}{N} \simeq (1 - \frac{1}{N}) \cdot (1 - \frac{2}{N}) \ldots\ldots\ldots \cdot (1 - \frac{k-1}{N}) = \prod_{i=1}^{k-1}(1 - \frac{i}{N})$.

Nelle ipotesi di N grande, 1-i $\simeq$ -i $\Rightarrow \frac{-i}{N} \simeq e^{-\frac{i}{N}}$, quindi ho $\simeq \prod_{i=1}^{k-1} e^{-\frac{i}{N}}$, ma questa è uguale alla somma degli esponenti $\Rightarrow e^{-\sum_{i=1}^{k-1}\frac{i}{N}}$. Ho inoltre che $\sum_{i=1}^{k-1} i$ è la somma di Gauss $= \frac{k\cdot(k-1)}{2}$ e quindi ho $e^{-\frac{k\cdot(k-1)}{2}} \simeq e^{-\frac{k^2}{2N}}$, approssimando k-1 a k. Questa è la probabilità di non avere collisioni: 1-p = $e^{-\frac{k^2}{2N}}$ da cui ln(1-p) = $-\frac{k^2}{2N} \Rightarrow$ k = $\sqrt[2]{-2N \cdot ln(1-p)} \Rightarrow$ k = $\sqrt[2]{2N \cdot ln(\frac{1}{1-p})}$.

Quindi all'aumentare del numero di messaggi k, aumenterà la probabilità di collidere. L'obbiettivo è capire quanti messaggi devo raccogliere per avere il 50% di probabilità di collidere:
$\sqrt[2]{N} \cdot \sqrt[2]{ln(\frac{1}{1-\frac{1}{2}})} = \sqrt[2]{N} \cdot \sqrt[2]{2}\ \sqrt[2]{ln2} \simeq 1.177\sqrt[2]{N} \simeq \sqrt[2]{N}$. Siccome N = 2^n, avrò k = $1.117 \cdot 2^{\frac{n}{2}} \simeq 2^{\frac{n}{2}}$. Se la RAND fosse una perfetta hash function: con 32 bit avrei 4.5 miliardi possibili output, e devo raccoglierne solo 60k per avere una collisione.
Per md5, con k = $1.8 \cdot 10^{19} = 2^{64}$ oggi è considerato weak, mentre per SHA256 ho $3.4 \cdot 10^{38}$.

4.5 PAP vs CHAP

Posso chiedermi quale fra i due è il più robusto. Bisogna comunque avere chiaro l'adversary model:

- eavesdropping attack: ascolto chi trasmette
- rubo i dati dal db

In PAP, se qualcuno ascolta il canale è finita, perché la password viene trasmessa in chiaro, quindi c'è la necessità di proteggere il canale di comunicazione (SSL, TLS, EAP/TTLS), ma nel caso in cui ci sia lo steal del DB PAP è molto più robusto, in quanto posso salvare le password non in chiaro. CHAP è invece meglio nel caso del 1° attacco, ma nel secondo no: non posso salvare l'hashing delle password, nel caso di PAP può essere effettuato brute force e la riuscita dipende dall'entropia delle password.
Perché in CHAP devo per forza salvare la password in chiaro: in CHAP la challenge è sempre diversa, non posso salvare H(psw, challenge) e se salvo solo H(psw), non posso ricavare la password perché la funzione non è invertibile.
Provo a modificare CHAP: faccio l'hash della password on the fly, ovvero faccio hash(hash(psw),challenge) e mando all'autenticatore, che ora può salvare l'hash della password. Ma in questo modo, se il db viene crackato, non devo nemmeno fare sforzi: userò l'hash della password per rispondere alla challenge e mi autenticherò.
In conclusione:

- Se l'attacco è sul canale di comunicazione, è meglio usare CHAP
- Se il canale è robusto ma il BD no, meglio usare PAP.

Quando valuto la sicurezza di un sistema devo capire bene cosa l'attaccante può fare e come posso difendermi.
Un modo per poter mitigare CHAP è aggiungere del "sale": authenticator mi manda la challenge più del salt, io prendo il salt e lo combino alla password e ne faccio l'hash, che uso per fare hash con la challenge.Cambiando il salt, anche il risultato cambia, quindi posso creare un DB con UID e l'hash di (psw,salt).Rimane comunque il problema in caso di db stealing, ma risolvo buttando via il db e ricostruendolo; sono inoltre soggetto a brute force e dictionary

attack. Ho bisogno di un DB aggiuntivo,che proteggo in maniera più forte, in cui salvare le password in chiaro per poterlo ricostruire in caso di steal.

4.6 Hash Chain

One time password: voglio una password diversa per ogni tentativo di autenticazione, così da essere al sicuro da reply attack. Sembra una cosa triviale: creo uno userDB con una lista di password random, per ognuna metto un flag che mi indica se è stata già usata o no, quando ne ricevo una la segno.
Su na scala reale: se ho molti utenti, il numero di password totali è considerevole, il problema non è tanto nella taglia del DB quanto nel dover cambiare la struttura del DB. L'idea è quindi di generare un numero random/pseudorandom di password da un seed. Uso una hash function crypto, come SHA256, a cui passo il seme e computo il digest. Parto da un seme P[0] e genero P[1] = H(p[0]) e così via, devo quindi salvare solo P[0] per poterle computare tutte. Uso P[0], poi P[1] etc..., ma il modo è errato: se riesco a leggere P[0] poi posso generare tutte le successive, quindi faccio il contrario: mando P[n], poi P[n-1]..., l'attacker non andare al ritroso nel calcolo (sto usando una crypto hash function), non è possibile invertire la funzione.
L'authenticator computerà da P[0] a P[n], ma su larga scala questo è oneroso: quello che viene fatto è computare offline, ade sempio durante la registrazione, fino a P[n+1] e salva solo questa. Quando riceverà P[n], farà P[n+1] = H(P[n]) e lo confronterà con il valore di P[n+1] che ha salvato. Il numero di password è finito, quindi dopo un po' sarà necessario rigenerare la chiave, per creare una nuova hash chain.
Posso avere un problema nel momento in cui ricevo l'ok per l'autenticazione, mando il valore successivo e non accade nulla: posso tentare le altre password, se si perde la sincronizzazione tra client e server, so qual'è ultima password correttamente ricevuta lato server (perché ho salvato P[n+1]) e quindi definisco una finestra di tolleranza per cui provo a fare hash per vedere se mi torna il risultato (la finestra va a salire), ovviamente il valore deve essere limitato.
Benefit della OTP:

- Invio in chiaro
- Rilasso la server security: l'authenticator salva solo la password che si aspetta di computare, quindi in caso di db steal non ho informazioni sulla password esatta.
- minore complessità del db

Problemi:

- Dimensionare bene n
- client side è vulnerabile, in caso di key steal è finita.

4.7 2-factor authentication

Non posso fidarmi della password dell'utente, quindi spesso viene inviato anche un codice (via sms, mail etc...), in modo che l'attacker deve trovare entrambe per poter avere successo. Il codice è un one-time authentication token generato su un device differente e ricevuto su un canale differente.
Deve essere human friendly: un codice da 6 a 8 cifre, possibile generarlo con un hash su cui poi viene effettuato un troncamento...
Se assumo che sia client che server sono sicuri, non ho bisogno di usare un hash chain: ho due protocolli possibili, HOTP e TOTP

4.7.1 HOTP-Hash One Time Password

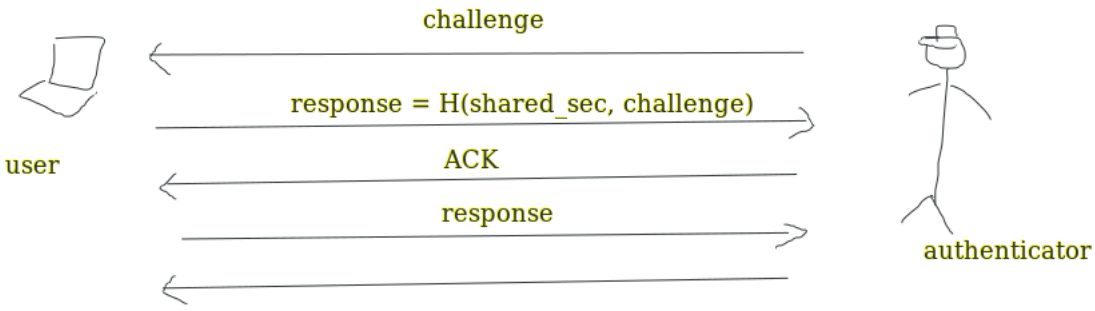
Ho client e server sicuri, c'è il segreto shared su entrambe, non computo P[n] = H(P[n-1]), bensì P[n] = H(segreto, n); ad esempio P[35] = H(secret, 35) e così via.
Anche se ottengo uno dei P[i] non posso ricavare gli altri se la funzione hash è crypto. Inoltre k può essere "infinito", parto da un counter e non devo precomputare nulla. Uso SHA256(k,n) che è un HMAC, e prendo il troncamento del risultato (6-8) digits.

4.7.2 TOPT-Time-based One time password

Sistema più sicuro, in cui non devo generare una OTP, am ha come assunzione che il tempo sia sicuro: ho un time sicuro, parto da un timestamp TS iniziale. TOPT = HOTP(k,T), dove T = $\frac{TS}{X}$, dove X è il range nel quale penso non avvenga un reply attack (solitamente 30 secondi). Questo TOTP ha valore per un certo lasso di tempo, computo il valore ad esempio alle 10:46 ed il server riceve alle 10:46, ma se c'è dello sfasamento il valore non torna. Per incrementare la robustezza posso provare ad usare valori precedenti, tolleranza ad esempio di uno slot temporale.
Se il tempo non è sicuro, un attacker può cambiare il tempo e riusare una OTP. Ad esempio: server NTP ha precisione di O(10 ms), quindi non è sicuro.

4.8 Mutual authentication con CHAP

Assumo che CHAP sia un protocollo sicuro, però è pensato per single authentication. Provo ad adattarlo per mutua autenticazione. Pro tip: non fare mai quello che segue, non si fa. Esce fuori un casino:



Non è una buona idea: uso la stessa chiave per rispondere alla challenge sia dello user che dell'authenticator, ma invece di essere l'utente il primo ad autenticarsi, chiede all'authenticator di farlo (posso farlo se il canale è full duplex). Se però la challenge è la stessa, non è detto che l'authenticator si renda conto che non è cambiata: quando ricevo la risposta posso compiere un reply attack, perché la challenge può essere uguale. Cambio il protocollo in un unico mutuo protocollo: l'authenticator manda il suo nome e la sua challenge, l'utente genera una nuova challenge, manda all'authenticator la nuova challenge e la risposta; ora l'authenticator può verificare che la risposta sia diversa.
Reflection attack: mando la challenge C_1, l'utente mi manda C_2 + hash per C_1. Fingo una perdita di connessione, sospendo la sessione e mando come challenge C_2, l'utente vede C_1 e C_2, ma non sa che deve verificare le due sessioni, quindi mi manda la risposta a C_2 e la nuova challenge C_2. Ora fingo che la sessione è tornata up e mando la risposta a C_2.
Ulteriore patch: ogni nuova sessione rende invalida la precedente, posso comunque compiere un man in the middle/intertwining attack. L'attacker prende il messaggio, lo manda all'authenticator e riceve l'autenticazione dal server, quindi fa credere all'utente che è connesso col server.
Per fixare: richiedo che venga effettuata una computazione sulla challenge dell'utente e dell'authenticator, ovvero di effettuare crypto binding sulle due

challenge. Lo user fa crypto binding su C_1,C_2 e si fa mandare dall'authenticator l'hash di C_2,C_3, ma così ci sono troppe challenge: l'attaccante invia C_1, mi faccio mandare l'hash di C_1,C_2 posso iniziare una nuova sessione con C_2.
La soluzione prevede che sia l'utente che l'authenticator usino le stesse due challenge, ma scambiando l'ordine con cui viene effettuato l'hashing,ma in questo modo ho progettato un protocollo diverso da CHAP.
Avevo due sessioni indipendenti, l'unico modo per renderle dipendenti è usare crypto dependency sulle due challenge.

5 Nonce

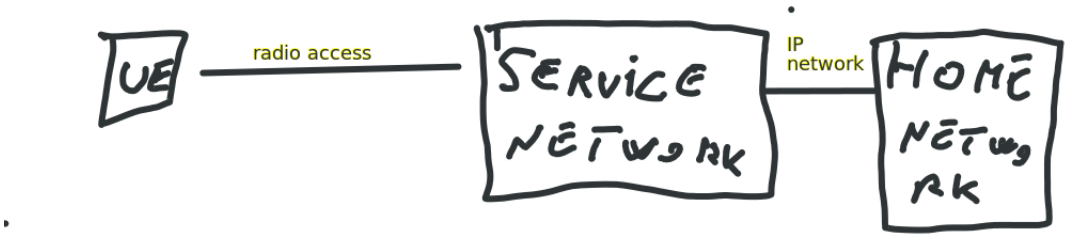
Una nonce è un valore sempre fresco, ovvero ogni volta diverso.
Sono di 3 tipi:

1. Random challenge: $\sqrt[2]{n}$ in termini di randomness
2. # seq : più robusto in termini di predicibilità, n.
3. timestamp: è predicibile, ma devo avere garanzia sul tempo (es: GPS e Galileo, GPS può essere spoofato).

La nonce è un superset di possibili challenge, può prevede l'utilizzo di più metodi

6 Challenge-response authetication in 2G/3G/4G(5G)

Architettura semplificata di un sistema cellulare:



La rete cellulare deve garantire almeno queste 3 parti, la serving network offre un servizio di roaming agli altri operatori(non è detto che sia lo stesso operatore dell'utente). l'autenticazione serve perché in questo modo il dispositivo può accedere alla rete e l'operatore sa chi sta accedendo. Usando un protocollo come PAP, la serving netowork vede la mia password e se sono in roaming in paesi molto ad est non so se esistono regole sulla privacy.
Non posso fidarmi della serving network, quindi uso un protocollo CHAP-like: la rete è complessa, la parte che gestisce l'autenticazione comunica con la home network.
In 3G, il mio device dice alla rete dove sono e chi sono, la serving network contatta la mia home network per ottenere i parametri di configurazione e a questo punto posso autenticarmi usando le credenziali con procedure crypto. In realtà, viene derivata anche la chiave per l'encryption: AKA = Authentication and key agreement, userò anche una chiave successivamente per criptare i messaggi.

6.0.1 Autenticazione in 2G

L'autenticazione è unilaterale: la SN manda alla HN l'IMSI che gli comunica il mio device (l'IMSI è il codice della sim) ed una challenge, ovvero chiede alla HN quale risposta deve aspettarsi dall'autenticazione dell'utente. La HN possiede l'id dell'utente e la password, riceve la challenge e ne fa l'hash usando il segreto, producendo l'SRES, fatta da un authenticator trusted: la HN è il ground truth. Inoltre, fornisce la K_c, ovvero la chiave temporanea che verrà usata dopo l'autenticazione per criptare i messaggi. La SN mi manda la challenge (128 bit random challenge in 2G), io (la mobile station) usa la funzione A_3 (simile ad un hash function) a

cui passa il segreto e la challenge. La risposta è di 32 bit e viene mandata alla SN, che controlla se è uguale alla SRES ottenuta in precedenza dalla HN. Sono protetto, perché la SN non conosce il segreto k_i (identity key) dell'utente.C'è anche la fase di key agreement: (k_i, rand challenge) $\longrightarrow$ k_c usata per criptare, schema di symmetric encryption.
In wi-fi: dispositivi che si collegano allo stesso AP condividono la stessa chiave di accesso, la protezione è solo dall'esterno, per la protezione interna servono ulteriori meccanismi (TLS,SSL,...) Nel modello appena descritto ogni utente ha una chiave diversa e questa chiave cambia per ogni nuova sessione.
La challenge è una nonce, con cui computo k_c mediante la funzione A_8 (anch'essa simile ad un hash function).
Se l'utente si collega da più celle, devo ogni volta ripetere il processo descritto sopra, quindi questo è molto lento. L'idea è quella di fornire alla SN un vettore di $<$ challenge, response, k_c $>$xN, in modo che la SN abbia N triple e questo porta a diversi vantaggi:

- viene contattata una sola volta l'HN, quindi pagherò il delay della connessione una volta sola
- la challenge random è una nonce che deve essere generata propriamente, se la genera la HN e non la SN sono più al sicuro.

Quindi lo schema di challenge-response:
challenge: RAND — secret: K_i — hash: algoritmo A_3. Gli algoritmi A_3 ed A_8 prendono 128 bit di K_i + 128 bit di RAND e restituiscono rispettivamente 32 bit di SRES e 64 di K_c (anche detto il segreto di Pulcinella). 2^{64} non è computabile, ma 2^{54} sì: la chiave K_c era di 54 bit, estesi a 64 con 10 zeri alla fine.

6.0.2 Scelta degli algoritmi

A_3 ed A_8 girano nel chip della sim. Ma io non ho accesso al chip della sim, quindi non conosco l'implementazione di A_3, ma non ne ho bisogno. Nemmeno la SN deve conoscerla, il risultato sta già nella tripla, è proprio la response, che è l'SRES, quindi ogni operatore può scegliere gli algoritmi che preferisce. Gli operatori scelsero di usare un algoritmo noto, COMP128 che non era open source, ma veniva tenuto nascosto $\Rightarrow$ security by obscurity. CI fu un leak del codice, e questo venne analizzato e violato da crypto guys molt forti in O(min), rendendo vulnerabili milioni di sim.
Morale:

- Security by obscurity non funziona, perché è difficile che se scoprono una vulnerabilità non la dicano.
- Algoritmo pubblico viene validato dai crypto shark che cercano di romperlo per il clout.
- Preferisci sempre l'open source al codice chiuso per la sicurezza

6.1 Autenticazione in 3G/4G

Il problema del 2G sta nel fatto che l'algoritmo per computare K_c era vulnerabile, ma non c'era nemmeno mutual authentication: suscettibile ad over the air attack, ovvero una finta base station a cui l'utente si collega. La base station non prova mai la sua autenticità, e non voglio questo. Uso un algoritmo open source per la mutua autenticazione: la mobile station comunica il suo IMSI alla SN, che lo manda alla HN e riceve una 5-pla < rand, XRES, C_k, IK, AUTN >xN.
L'IK è l'integrity key, usata per garantire l'integrità del messaggio. Questo perché l'encryption non la garantisce, quindi serve una chiave diversa dalla K_c per garantirla.L'AUTN serve invece per provare l'autenticità della rete all'utente, è il Network Authentication Token.
La SN mi manda l'AUTN e la rand, provandomi di essere trusted, ma l'AUTN è stato prodotto dalla HN, quindi voglio che sia il device a produrre la challenge che la SN dovrà risolvere. In questo caso non è così, dovrei avere due nonces, uno dall'MS alla SN ed uno dalla SN alla HN.
Funzioni usate:
f_2(K, RAND) = 32 bit di RES
f_3(A_8 equivalent)(K, RAND) = 128 bit di C_k
f_4(K, RAND) = 128 bit di IK
Tutte dipendono solo dal segreto dell'utente e dalla random nonce, le implementazioni sono note.
Sarebbe possibile autenticarsi con un solo messaggi, usando il timestamp:
se la mobile station e la SN usano ad esempio GPS, sotto l'assunzione che il tempo sia sicuro, conoscono perfettamente la nonce usando TS.
Farò H(TS,K), non posso avere reply attack etc... e con questa forma di nonce evito l'uso della challenge.
La mutual authentication in 3G+ (simile anche in 4/5G) prevede che la MS invii una nonce, invece di usare una quantità random, usa un #seq number: in questo modo posso sapere quante volte ho fatto un accesso e qualcuno nella rete mi dice che mi sto autenticando per la #seq + 1 volta. Se mi arriva un messaggio con un #seq vecchio, scopro che è un reply attack. Se il vece il #seq è più grande anche solo di 1, va bene (definisco anche in questo caso una tollerance window): i numeri di sequenza della MS e della HN devono essere sincronizzati, perché la SN si autentica alla HN per ottenere il vettore di credenziali.Quindi, quando mi autentico, uso il #seq come challenge implicita, risparmiando un messaggio: il messaggio che mi fornisce la SN è un'operazione della nonce + k, usando le credenziali fornite dalla HN; in questo modo so che la SN ha le mie credenziali. È un 2-way exchange con 2 messaggi, il problema è che la MS e la HN devono essere sempre approssimativamente sincronizzate; se si perde la sincronia, servono dei meccanismo per ripristinarla.
Format dell'AUTN:
N° sequenza a 48 bit — AMF: 16 bit di auth and key management — 64 bit di MAC-A, derivato come segue: MAC-A = f_1(k, SQN, AMF, RAND), la coppia SQN + RAND corrisponde ad un crypto binding, K ed SQN sono la proof of

knowledge di k, l'AMF sono informazioni aggiuntive.
Una volta connesso alla service network, questa mi manda un TMSI, ovvero un identificatore temporaneo allocato dinamicamente quando mi collego; nelle prossime autenticazioni userò questo TMSI (GUTI in 4G). Il TMSI è meglio per la privacy, in quanto se mi collego usando sempre l'IMSI, posso essere tracciato, invece qui uso una quantità che via via cambia.
L'unica vulnerabilità è che la prima volta l'IMSI viene mandato in chiaro, bisogna cercare di usarlo il meno possibile.
Mi autentico ed ogni volta che mi ricollego cambia il TMSI, occorre fare molto lavoro aggiuntivo per evidare che i TMSI siano legati fra loro. Devo inoltre proteggere il sequence number SQN: potrei non trasmetterli ed usarli davvero come informazioni implicite, oppure produrre un encryption con la chiave, ma prima del collegamento non la ho: se però sono autentico ed anche la SN lo è, allora vuol dire che entambi conosciamo k, quindi possiamo derivare qualcosa da k. Faccio l'encryption del SQN con un pattern AK apparentemente random: rendo AK computabile per entrambe gli end, quindi poi la base station potrà risolvere:

- leggi random
- computa f_5(k, random) = AK di 48 bit
- de-anonimizza #seq : #seq $\oplus$ AK $\oplus$ AK = #seq
- leggi il resto del pacchetto
- computa f_4(#seq , k, rand, AMF) = MAC-A
- controlla il MAC-A

7 Pro-tip: come generare password a partire da un segreto master

Ho il seguente problema: devo generare chiavi infinite per infiniti utenti: posso usare un PRNG e mettere i record userID — password in un database e proteggere il DB. Pro tip: uso un master secret S, che tengo al sicuro, e quando devo generare una nuova chiave per l'utente uso un identificativo univoco per l'utente (es: il codice fiscale) e faccio hash(S, UID).

8 Message authentication-Integrity

In 3G e oltre ho l'IK per l'integrità del messaggio, faccio quindi messsage authentication. Ricordo che la confidenzialità è diversa dall'integrità: con la prima,voglio nascondere il contenuto del messaggio mentre con la seconda voglio che il messaggio non sia modificato durante la trasmissione, solo la sorgente legittima dovrebbe poterlo forgiare.
Ho bisogno di un algoritmo che garantisca l'integrità.

8.1 Message Authentication con symmetric key

Il sender ed il receiver che hanno una stessa chiave k, ad ogni messaggio aggiungo un TAG = gen_tag(k, message). Il messaggio ha una size arbitraria, ma il tag deve avere size fissa, quindi userò qualcosa di simile ad una funzione hash. Il receiver riceverà il pacchetto e ricomputerà il tag, confrontandolo con il tag ricevuto.
esempio: message authentication code (MAC) è più debole della firma digitale
La firma digitale non può essere contraffatta, nessuno può modificare un messaggio firmato da me. Nel caso del tag sender e receiver possono modificare il messaggio, chiunque possiede k può farlo. La digital signature ha la non repudiation property o source authentication. Ad esempio, in una chat multicast si usa la stessa IK, quindi chiunque può produrre un messaggio spaccandosi per me, con la firma digitale questo non può accadere.

8.2 Message Authentication con hash functions

Ho mai detto che una hash function può essere usata per msg auth?
Nuovo problema: come usare hash function per msg auth e ci saranno problemi (perché non è quello il purpose per cui è pensata).
Encrytpion non garantisce integrità a meno che si usi un authenticated enrcyption ⇒ AEAD algorithms, Authenticated Encryption Associeted data ovvero un algortimo che fa sia encryption e authentication.
In TLS 1.3 (la nuova) hanno proibito di usare algoritmi che non abbiamo authentication, quindi sono AEAD.
AES-128 o AES-256 è enrcyption only, AES-GSM o AES-CCM sono auth enrcyption.

8.3 Message authentication with simmectric key

Prendi msg m, computa con una chiave k nota ad entrambi gli end(nota ⇒che è pre-shared) C'è una funzione che è usata per generare il tag: riceve una size arbitraria e produce un tag di size fissa e possibilmente piccola (non troppo, per birthday paradox). Trasmetto msg + il tag, message authentication code aggiunge bytes al msg, c'è dell'overhead in quanto non deve aver infromazione(il msg in se è al massimo livello di entropia). Recevier verifica il tag usando la stessa funzione, nota e condivisa, generando il nuovo tag dal msg + chiave k e lo confronta con quello ricevuto.

8.4 Definizione di sicurezza per Message Authentication Code

IND-CPA model definiva la confidenzialità, posso trovarne uno analogo per msg auth?

Sicurezza in integrity vuol dire che l'atk non può essere in grado di creare un nuovo msg o poter modificarne uno; anche se il msg modificato perde di senso è considerata una violazione.
Formalmente, faccio un "gioco" contro l'attaccante:

- attacker model può essere Known Message Attack o Chosen Message Attack, ovvero attacker può chiedere qualsiasi coppia (msg,tag) precedente
- può essere adattivo ovvero che il msg è scelto dopo una analisi della situazione.

Ora, se l'attacker scegli uno nuovo messaggio m, diverso da quelli del passato per cui ha i tag, non deve poter forgiare il nuovo tag per il msg m.
Formalmente, la probabilità di forgiare una coppia valida deve essere un ϵ(prob dell'ordine di 2^{-100}):

- Devo escludere che il tag sia di 1 byte
- Non può tirare a caso il tag del msg con scelta puramente random. Se fosse di 1 byte $\Rightarrow$ avrei $\frac{1}{256}$, che non va bene, il minimo è almeno 96 bit di tag (meglio 256).

Differenza cruciale nella scurezza: IND-CPA l'attacker poteva scegliere se il msg era A o B e aveva esattamente $\frac{1}{2}$ possibilità.
Message integrity protegge dal man in the middle? Sì, genero il msg m, produco il tag=F(K,m). L'atk intercetta il mesaggio e vuole cambiarlo: se F è cryptographically strong:

- K non può essere computata dal msg e dal tag.
- Non posso cambiare il tag in un nuovo tag senza conoscere k, non posso computare tag*=G(K,m*)
- Non posso cambiare m in m' così che F(K,m)=G(K,m')$\Rightarrow$ anticollision property.

Se lo schema è sicuro, allora potrò sempre intercettare un mitm atk.Mitm ha due aspetti:

- networking class: triviale farlo,ARP poisoning, DNS spoofing.
- L'attacco è efficace se posso modificare il msg, non solo cambiare il flow dei msg.

Un buon algoritmo deve anche proteggere dalla creazione di un nuovo msg: message spoofing$\Rightarrow$ creo un nuovo messaggio in cui metto un ip fake facendoti credere che è quello con cui vuoi comunicare.
Posso risolverlo con un auth mechanism:

Se ogni msg è autenticato: DNS è autenticato in plaintext, come faccio a sapere che è proprio, es. Google.com?
Devo aggiungere qualcosa che mi garantisce che sia Google ad esempio con un tag.(la versione di DNSSec dovrebbe proteggere da questo, ma questo aggiunge complessità alla rete quindi si continua ad usare DNS.)Posso spoofare msg, ma devo conoscere il tag⇒se algoritmo è buono probabilità è un ϵ.
Questo schema NON protegge da un reply attack:
voglio mandare due messaggi, es due transazioni. Produco due msg identici, ma la F si applica alla chiave⇒la F deve essere deterministica (va ricomputata all'altro end)e quindi i tag saranno gli stessi,MAC non è abbastanza.Ma se i messaggi hanno un contenuto diverso: timestamp, num. seq etc.. potrei dire che non ci sono problemi.Ma non è così: l'applicazione dovrebbe essere disegnata senza avere in mente problemi di sicurezza.Il protocollo deve essere sicuro, non mi deve importare dell'applicazione.
Prevengo reply atk: uso le nonces, devo garantire a livello di protocollo che tutti i messaggi siano diversi, aggiungo una nonce ai msg. Computo il tag sul msg+nonce, posso mandare la nonce in chiaro.

- Se uso seq num: come gestisco i reboot?Devo prestare attenzione. Parto da 0 e vado avanti, però perdo alcuni n° sequenza, come faccio a dire che i pacchetti ricevuti con alcuni buchi in mezzo sono ok? Devo tenere in mente l'utlimo correttamente ricevuto per discriminare reply atk.
- Random number, se truly random sono meglio.Non ho probelma del reboot, ma come controllo se pkt è nuovo? Ho un certo n° bit,quindi dovrei tenere tutt la lista de msg precedentemente ricevuti, costo di memoria e di computazione per il controllo.
- Timestamp migliore possibile, ma il tempo deve essere garantito o ho problemi.

Settare una nonce sembra facile ma non lo è, la maggior parte dei probelmi implementativi è qui.
1° ingrediente:
Hash functions: molto veloci, sono anticollsione se cryptographic. Buoni prodotti:

- SHA-2 family(SHA256, SHA224,SHA384⇒SHA512 troncato, SHA512). Nel passsato SHA1 e MD5, MD5 la più comune e famosa funzione hash,oggi tutte e due rotte.
- Next: SHA-3 family, sempre gli stessi digest ma con approcci differenti.

es: in TLS e Ipsec, SSH non troppo serio si usa SHA256, sha256sum fa hashing di file su Linux.
2° ingrediente:
Includo il segreto nell'hashing del messaggio messaggio. Facile? Ma dove metto l'auth key nel msg?Lo metto dopo il messaggio: H(M||K), o faccio il contrario?

O in altri modi? Ad esempio metterlo sia all'inizio che alla fine etc..Perché me ne preoccupo?
Una funzione hash teorica è una black box, c'è anche definizione per la perfect hash function:
Random Oracle: black box, che preso input X, H(X) = valore truly random, ma che si ripete se X è lo stesso. Ma le due cose non possono coesistere, H(X) deve essere computabile. Nella teoria questo è il modello ideale (come per one time pad) che vorrei avere, ma non posso implementarlo.
Devo vedere nel box:tutte le hash functions (tranne SHA-3, oggi non usate) sono costruite con la costruzione iterative Merkle-Damgard: è difficile trovare f tale che: f(any size)$\longmapsto$ fixed size. Ma è possibile trovare f t.c:
f(fixed size)$\longmapsto$ samller fixed size otuput. Compression function, che possono essere molto buone.
es: sha256
prendo msg di k bit, paddo il messaggio in modo che il risultato(compreso i 64bit di lunghezza del messaggio) sia multiplo di 512 bit: se ad esempio la size del mio file è 1025 bit, metto un bit ad 1 seguito da vari zeri, alla fine del msg mette la size del msg come lunghezza modulo 2^{64}, sono 64 bit (faccio il modulo nel caso in cui lunghezza sia maggiore di 2^{64}, così che sia di size fissa). Ora taglio il msg in chunks di 512 bit: parto con un initialization vector(non crypto) che è noto e fisso, deve poter essere ripetuto. SHA256 prende IV 256bit,diviso in 8 gruppi da 32, è una costante.L'IV fa sì che la funzione di compressione prenda 512(il chunk) + 256(l'IV) = 768 bit di input.Questo perché SHA256 usa aritmetica mod 32 o 64 a seconda dell'architettura.La compression function comprime i 768 bit in 256 bit che è l'hash summary del chunk 1.
Ma ora, se uso questi 256 bit come input per un secondo blocco di compressione, che comprime il chunks 2? SHA256 reitera la stessa funzione di compressione.
La F è il cuore dell'hash function, theorem di Merkle-Damgard dimostra che se F è resistente, ovvero soddisfa le 3 proprietà di una funzione hash⇒l'intera costruzione è sicura.(la F non deve essere lineare)
La chiave è trovare una buona compression function, questa prende un input fisso e ridà un output fisso, a questo punto posso usarla iterativamente; l'ultima iterazione mi darà i 256 bit finali.
In che posizione metto il segreto nell'argomento dell'hash fucntion? Prima del messaggio, o dopo, o in altri modi? La posizione del segreto conta ed è importantissima:
es: msg di 1GB, segreto 128bit, poi ho pad+length.Messaggio è noto, vedo il tag = hash(msg,k), vado da 0 a 2^{128} e faccio H(msg,k_x)=?tag. Brute force atk devo computare fino al massimo 2^{128} hash functions.
SHA256 è white box, so che è costruita iterativamente, il msg è sempre lo stesso: computo i primi blocchi che contengono il messaggio e prenderò l'output precomputato (i 256 bit risultanti), ed ora dovrò computare solo l'ultimo pezzo a partire dal precomputato.Non quindi computare N$\cdot$ 2^{128} blocchi, bensì 2^{128} $\Rightarrow$ riduco la complessità d un fattore N.
Se metto il secret all'inizio, posso rompere la forgiability?Posso forgaire un tag valido per un m$^{'}$ scelto da me, partendo da M,tag=H(s,m). Sì è possibile:

triviale forgiare un messaggio autenticato valido m' != m. Estendo msg, che può anche essere insensato, con una parte di plaintext.
Non posso modificare il msg originale ma non è un problema, inoltre lo faccio senza conoscere il segreto: es. aggiungo una transazione alla fine del messaggio.Aggiungo extra chunks, partendo dal MAC di prima e genero un MAC extended valido.
Questo è un problema ⇒ ho una funzione forte, ma la costruzione rompe tutto (errore tipico della crypto), quindi non si usa mai una funzione non pensata per quel purpose, anche se i purpose sono simili.
La posizione del segreto CONTA TANTISSIMO.
Come fixare il problema:
Hash Based Message Authentication Code (HMAC), che è stata dimostrata essere sicura come l'hash sottostante.
Ho imparato che una secure hash non basta, quindi HMAC aggiunge un modo sicuro di aggiungere segreto nell'hash, non patcho l' hash in se quindi non dipende da come è fatta l'hash.
1996, paper di Bellare, Canetti e Krawczyk con due versioni: crypto e IETR RFC 2104.
Pluggable hash e usando l'HMAC non aumenti il costo computazionale di molto:
$HMAC_k(M)$=H($K^+ \oplus$opad |H($K^+ \oplus$ipad|M))
Il primo pezzo contiene la chiave, i secondo il messaggio. Sembra che sto facendo come prima, ma in realtà sto usando hash del messaggio tra message e secret alla fine. Quindi faccio hash della chiave seguita da hash di message e chiave,come fare 2 volte hash del msg.
Se il segreto K è < della lunghezza di un blocco fai si che sia di pari lunghezza, paddo con zeri, ottengo così K^+.Questo è il primo chunk di SHA256.
Per la sicurezza della costruzione, i due segreti che uso negli hash devono essere diversi: miglior costruzione è la nested MAC construction : H($secret_1$ || H($secret_2$ || msg)). Ma chiedere di usare due segreti sarebbe stato un disatro, quindi per praticità non era conveniente lasciare all'implementatore la scelta dei due segreti.
Soluzione è che produco due segreti dviersi a partire dallo stesso: in entrambi i due risultati flippo bit diversi riseptto all'originale, sembrano quindi due segreti indipendenti(ma non lo sono) ed hanno una distanza larga in termini di bit.
es : k = 01010101, inner: 01010101$\oplus$01011100=K_i, outer: 01010101$\oplus$00110110=K_o (entrambe le sequenze ripetute come serve).
Parto dal msg, aggiungo all'inizio (prefix) K_i, runno hash function: parto da IV e lo unisco a K_i ed ottengo un secret IV.Hash sugli altri chunks, ed ottengo l'inner hash: ho un classico MAC secret prefix, devo mettergli una pezza: prendo l'oueter key K_o e faccio hash del singolo blocco (inner hash + pad).
Ottengo quindi HMAC, che è dimostrato essere una costruzione sicura.
storiella: 2005 md5 broken, tutti gli HMAC tags usavano md5. Thm ti dice che la costruzione è sicura quanto l'hash sottostante: se l'hash è unsecure ⇒dovrebbe rompersi anche il meccanismo di HMAC. 2006: non era ancora stato trovato un atck pratico ad HMAC di md5.
Assunzioni: modello math dell'hash function:

- pseudorandom output
- anticollision property.

Entrando nei dettagli, Bellare si rende conto che non usa mai la proprietà 2 e capisce che HMAC è più sicuro dell'hash fuction, finché la properietà 1 non è violata.
Paper del 2006 su collision resistance NON necessaria.
Messaggi importanti:

- Confidentiality != integrity
- Message authentication with symmetric key
- Reply atck: MAC non è abbastanza, servono nonces e vanno gestite bene.
- Crypto hash functions
- Come includere key nell'hash fuction? Non è triviale, usa HMAC.

9 Gestione dell'accesso remoto: RADIUS

Tool usato nel backend, Remote Authentication Dial In User Service, obsoleto: oggi migliori protocolli(DIAMETER) ma ci sono un sacco di problemi quindi è utile studiarlo.
Posso accedere alla rete usando diverse tecnologie, tutte eterogenee fra loro e largamente distribuite. Gestire la rete con tutte queste tecnologie ed access point: uso server centralizzato, RADIUS server che è incaricato di gestire username e password dell'utente, così da evitare la distribuzione all'interno della rete.
Anche una questione di sicurezza:(di solito in AP: Linux machine con db interni), non lascio username e psw distribuite in giro per la rete.
Devo cambiare l'authentication model: faccio auth con local technology, RADIUS client che counica con l'utene e col server contatta quest'ultimo ed il server ,manda RADIUS response con un si o no a seconda se l'utente può accdere o meno⇒parte più importante.Il client dice quindi all'utente se può entrare o no(l'utente non sa che sta usando RADIUS).

9.1 RADIUS: AAA protocol

3 servizi di solito eseguiti insieme:

- Authentication
- Authorization: da non confondere con Authentication, qui voglio sapere che l'utente ha il permesso di usare il servizio (perché ha pagato o per altri motivi). Posso avere

  - authentication senza authorization
  - authorization without authentication ed avrei un servizio privacy preserving.
    Letteratura scientifica è ricca di tecniche per farlo, ma nel mondo pratico non molto usato.
  - l'intersezione fra i due.

  Serve per management

- Accounting: transmitted bytes (quanti GB sto consumando), billing, minuti di telefonate spese etc..
  Segno cosa stai facendo in termini di una risorsa che stai usando.

9.1.1 RADIUS è client-server protocol

Richiesta parte dal client, non confondere il RADIUS client con l'end user, ovvero il NAS: ho end user - NAS- RADIUS client- Server.
Basato su UDP/IP porta 1812, client port è ephemeral. Sistema centralizzato, logicamente centralizzato: in teoria ho un singolo server ma in pratica è ridondato (sennò è single point of failure)
In RADIUS si può usare roaming: se cambio città rispetto a dove sta il server, es. della mia università, dovrei cambiare account, ma quello che accade è che la mia richiesta viene presa dal RADIUS server della città e la inoltra al RADIUS server della mia univeristà, agendo da proxy server.
Architettura complessa, diversi blocchi:

- Server application
- User db: per ogni username ho almeno authentication info, authentication method e authorization attributes
- Client db: clients che possono comunicare col server.
- Accounting db: se RADIUS usato per accounting, deve essere aggiornato in real time, per questo separato dal db utente.Non necessario se si fa solo authentication.

9.1.2 RADIUS security features

Due feature, 1° è per packet authenticated reply: NAS non ha le mie credenziali, le manda al server, atck interecetta il messaggio e risponde con un "sì", il NAS ora vede che l'utente è autenticato.Non devo pter spoofare il msg⇒deve essere autenticato, ed è quello che è stato fatto: si usa shared secret, approccio CHAP-like,ma:

- solo la reply è autenticata
- l'autenticazione è hash based e non HMAC-based

- funzione hash specifica MD5, quando uso una hash function deve essere future-proof, se metto uno specifico crypto algo in un protocollo è male: qualcuno prima o poi lo romperà. Non è semplice andare poi a modificarlo. Il protocollo è una cosa, l'algoritmo di encryption deve essere messo a parte, così da cambiarlo in caso venga violato.

- Secret non truly random, ma low-entropy shared key

2° servizio: user password enrcyptata: se uso PAP, ho la psw in chiaro. Standardizzazione di un meccanismo. Problemi:

- Custom mechanism, non inventare algoritmi per quanto possibile, ma usane uno già esistente. (Non era rotto, però devo considerarlo come possibile vulnerabilità).

- Shared secret key usata anche per l'authentication ⇒NUN SE FA, anche se non è exploitabile è errato, perché se rompi la chiave rompi più di un servizio.

9.1.3 RADIUS authenticated reply concept

End user credentials $\Longrightarrow$ manda le credenziali al NAS, RADIUS client e server hanno uno shared secret che è $\neq$ dalle credenziali del utente. NAS parsa le informazioni e le traduce nel RADIUS language, include le credenziali in un pacchetto RADIUS che è un pacchetto UDP/IP che ha:

- ID field: mi permette di matchare una richiesta con la risposta.

- Authentication field: nonce di forma strana, è una nonce che mando al server così che il server possa creare un reply message (sì, no go-on se servono più informazioni) e possa autenticare il pacchetto, ovvero il pacchetto deve avere un authentication tag. In message authentication includevo il TAG (che era HMAC di K + content), qui ho una cosa analoga: ho la risposta, il tag si costruisce combinando l'ID, il valore random usato come nonce ed il segreto pre-shared.MAC=H(ID,nonce,secret).
  Il reply può anche avere authorization, esempio poter permettere accesso per un tempo limitato.

NAS si tiene in un local db l'associazione ID-nonce(authentication). Faccio un check e se mi torna ⇒ sono sicuro che il messaggio mi è arrivato dal server e so che non può essere replicato perché l'auth è fresh per ogni nuovo handshake.Ora NAS passa l'informazione all'end user. È una sorta di challenge-response:

- la challenge è il request authenticator

- la risposta include anche,una volta validata, il messaggio di risposta.

Formato del pacchetto:
IP header | UDP header | RADIUS packet:

- byte di codice:
  - 1) sì
  - 2) no
  - . . .
  - 3)access challenge: sta per go-on, non inteso come la classica challenge.
- 1 byte di identifier
- 2 byte di length per il pacchetto
- 16 byte di authenticator che deve essere non replyable ⇒ unique. Sono 128 bit ⇒ 2^{128} possibili authenticator, se fosse realmente truly random, avrei avuto probabilità di collidere proporzionale al birthday paradox (ordine 2^{64}).
- Attributi sono triplette di (type,length,value), ogni tipo corrisponde ad un determinato tipo (username, password, framed-MTU, Callback-number)

Authenticator field: la parte più importante per la sicurezza.Dovrebbe essere unico ed unpredictable per evitare reply attack. Ha due scopi: nell'access request server per authentication mechanism, nella response è sempre di 16 byte ma viene usato per il TAG. TAG è MD5(Code|ID|Length|RequestAuthenticator|Attributes|Secret): qui code è codice di risposta, length è la lunghezza del pacchetto di risposta, attributes sono le triplette. Request Authentication si ottiene dall'access request. Access-request di solito contiene 2 classi di informazioni, uno dell'utente ed uno dell'access service device:

- Username: NAS ha le credenziali, deve mandarle al server
- Password dell'utente
- Identificatore del RADIUS client, NAS-IP o NAS-identifier
- Identificatore della porta a cui l'utente sta accedendo, la NAS-port (se il NAS ha una porta)

Access-reject: o ho fallito l'autenticazione oppure non ho l'autorizzazione (esempio: non ho pagato)
Access challenge è un go-on message: usato quando server vuole che venga fatto altro: ci sono altri protocolli di autenticazione (esempio: EAP-TLS, EAP-TTLS) in cui devo fare più operazioni, che richiedono più messaggi

9.1.4 PPP CHAP support with RADIUS

In una situazione normale di challenge handshake ho user, server: server mi da challenge,rispondo e lui mi dice si o no.
Nel caso di user | NAS | server:

potrei generare un processo simile, ma se faccio questo devo anche mandare il segnale fisico per far capire che l'utente è attivo: overhead grande, devo "svegliare" l'utente, il NAS deve chiedere la challenge al server e così via.
L'utente si sveglia, il NAS genera la quantità random (mi dovrei fidare dell'access point): utente risponde con hash della password e della challenge usando CHAP.
Il NAS crea Access-request RADIUS con Username|Risposta della challenge| Chalenge|Servizio....
Ora il server può verificare se il client è autentico e decidere se dargli accesso o no, manda RADIUS Access accept. Nel caso di protocollo CHAP non uso access-challenge message, uso solo Access-request.
Vulnerabilità: messaggio del NAS non è autenticato, l'Access Accept non contiene la tripletta di username o psw, è anche vero che la challenge cambia sempre.NAS non può verificare che la challenge era quella vera. Attacco:
prendo il NAS, mando una challenge "1234" e user manda reply"$\alpha\beta\gamma$" NAS manda il pacchetto al server ed ottiene Access Accept.
L'attacker si finge me: prende il pacchetto che ha generato fingendosi me e sostituisce ai campi dell'auth che il NAS gli ha mandato e la sua risposta alla challenge (che è random,tanto non è importante che sia corretta), a quel punto lo invia al server e non è detto che il server faccia un check per vedere se la challenge che il NAS mi ha dato è fresh o no. Attacco al payload del messaggio: rispondo con una coppia di valori precedenti validi.
Dal 1998 anche le richieste diventano autenticate, ma non era una cosa necessaria.
Problema: posso fixarlo? Potrei pensare di autenticare reply e request, ad esempio fare HASH(request, reply).

9.1.5 Password encryption

Se user manda username e psw con PAP: NAS dovrebbe mandare nel RADIUS packet, ma sono in chiaro. La rete in generale, tra il NAS ed il server RADIUS non può essere trustata ⇒ tecnica per criptare la password: predo la psw nativa, la paddo per riempire un blocco da 16 byte, faccio MD5(secret|RequestAuth), risultato sembra una string pseudoranom, quindi uso una tecnica simile allo stream cipher: il keystream non è prodotto da uno PNRG, ma da un hash function. Psw è messa in XOR con il keystream ottenuto dall'MD5(secret|RequestAuth).
Se la psw è più di 16 caratteri: posso dividerla in due blocchi e paddarla con lo stesso valore, ma il segreto è lo stesso e c'è una sola nonce ⇒ padderei due volte con lo stesso keystream. Computo un keystream differente, usando il cipertext precedente e faccio XOR con i due blocchi in cui divido la password.

9.2 RADIUS Security Weakness

Vulnerabile al message sniffing e modification. Access request non è autenticato, il testo è mandato in chiaro quindi ho problemi di privacy.
Soluzione non c'è, devi coprire con un altro protocollo (ad esempio TLS), per l'autenticazione usato EAP (Exstensible Authentication Protocol): protocollo

che permette di scambiare messaggi di autenticazione, difatti nella specifica si trova EAP-TLS, EAP-AKA, ovvero usi un protocollo di autenticazione con dentro un AEP packet exchange.
Message authenticator: ho un pacchetto di richiesta: contiene code|ID|Length|RandomAuth|triple(T,L,V) devo aggiungere un TAG, l'idea è di creare una nuova tripla T,L,V in cui il tipo fosse sepcifico per l'autenticazione. Il valore ora è computato con HMAC-MD5, type è 80 e lunghezza 18.
Reply atck: evito reply attack al pacchetto RADIUS di base, ma posso fare reply di una richiesta. Il pacchetto contiene una nonce e l'auth TAG, ma questo è un pacchetto valido, quindi posso replicarlo. Per evitare reply attack di request message, il server deve verificare che la nonce sia fresh. Può o non essere un problema: separa la practical explanation dalla vulnerabilità, deciderà chi implementa se questo è un problema o no.

9.2.1 Dictionary attack to shared secret

Problema grande di RADIUS, cos'è lo shared secret? Segreto che sceglie il network manager, problema è che è difficile che venga inserita una stringa truly random, ma una stringa a low entropy, ricorda inoltre restricted charset. Spesso un singolo segreto è usato per tutta la rete esempio: Fonera, aggregazione di AP a cui si ci può connettere in roaming. Stesso segreto per 100k+ device ed era triviale (tipo Salute! in spagnolo).
Quindi, usare uno shared secret per ogni client (metodo del segreto unico, che conosco solo io e ne faccio HMAC con un identificatore univoco dell'AP).
Possibile fare dictonary attack offline:
intercetto una coppia (request,response), ho tutte le info per fare brute force o dictionary atck e posso fare precomputation perchè il segreto è alla fine nell'MD5 del response packet.
Se richiesta e risposta su due canali diversi, e posso accedere ad esempio solo la request: non serve la coppia. Siccome il segreto è lo stesso mi basta generare uno userID ed una psw arbitrari, so che avrò una risposta con i campi definiti. Prendo la nonce dal request packet, fare nonce con la psw che ho scelto (Chosen Plaintext atck), quindi ho un keystream e posso fare bruteforce con dictionary atk.
Attacco alla password dell'utente: parto dl nome della vittima che voglio, metto psw arbitraria, ottengo unser password attribute e la psw encryptata che è scelta da me, pulisco encrypted password ed ho un keystream valido. Suppongo di voler fare brute force di un utente: faccio trial di psw, ma è lento e verrei bloccato dopo un certo n° attempts. Ma così ho trovato il modo di bypassare il server: mi metto dietro il NAS e spoofo tutta una serie di request (non è detto che il server faccia check che la nonce sia diversa) e faccio dictonary attack.

9.2.2 Poor PRNG implementations

PRNG è una delle parti più importanti in security.Security in RADIUS richiede un Request Authenticator unico e fresh: ho un req auth di 128bit, 16 byte.

esempio, prendo un random generator, lo chiamo rand(), genera 4 byte:

- Lo chiamo 4 volte.
- Lo chiamo una volta e riempio di 0
- Faccio md5() del risultato della chiamata.

Quale meccanismo uso? PRNG ha un periodo, rand() ha un periodo di 2^{32}: periodo è la lunghezza del ciclo affinché non si ripeta lo stesso pattern (in molti casi, per non crypto PRNG il periodo è 2^{n_bit}). Mando il RADIUS packet e l'auth req. non dovrebbe ripetersi. Se faccio merge di più pacchetti: il periodo si accorcia, perché abbiamo preso più valori. In termini di entropia, 2 e 3 sono quasi equivalenti: sono sicuro se la nonce non si ripete, l'approccio 1 ha 2^{30} come periodo, mentre 2-3 avrebbero la stessa sicurezza.
La maggiora parte delle implementazioni di RADIUS usano non crypto PRNG. Se uso PRNG che è buono dal punto di vista statistico, ma può non essere dal punto di vista della sicurezza:

1. Predictability: non devo poter predirre quale sarà il prossimo valore
2. Periodo: prima o poi il generatore si ripete, non voglio short cycles.
3. Random generator garantisce valori unici o ripetuti: ci sono alcuni random generator in cui è possibile garantire che se genero blocchi di dati, questi sono diversi. es: AES ha blocchi che non sono ripetuti

Riguardo al ciclo:
Linear Congruential Generator: $R_{n+1} = (a \cdot R_n + b)$, nel caso di rand a e b scelti in modo che il ciclo sia di 2^{32}, nel caso di questi generatori se conosci un valore li conosci tutti.
Mersenne Twister: 2^{19937}-1 è ciclo "infinito", ma i valori si ripetono.
Se so che i valori si ripetono, al sicurezza è $2^{\frac{N}{2}}$, altrimenti è 2^N.
Ora che so che RADIUS ura poor PRNG, mi aspetto che auth request ripete: stesso problema di WEP, posso avere più o meno predicibilità e penso ai possibili attacchi. Sono tutti reply attack: monitoro un certo n° attempts in cui ho utenti validi, ogni richiesta avrà una risposta con delle nonce. Creo tabella: Auth request nonce|Access accept packet. Access accept packet mi da il permesso di accedere al sistema. Creo dizionario, dopo un po' entro nella rete, NAS gemera una nuova access request che può contenere un numero che già è apparso, faccio reply di una risposta positiva e rispondo ⇒ ho accesso alla rete.
Stesso alla user psw: è encryptata con MD5(segreto, auth), se auth si ripete il keystream è lo stesso ⇒ two time pad e posso romperlo. Creo dizionario di request auth|user psw $\oplus$ MD5(secret, nonce).Raccolgo il cipher text, quando avrò la ripetizione (di uno stesso keystream con una psw diversa), faccio XOR e ottengo lo XOR fra due password e sfruttando la low entropy le ottengo entrambe.
Posso anche spoofare le password, incrementando il dizionario: aiuto un attacco passivo, uso psw finte che conosco ⇒ ottengo la mia psw in XOR con il

keystream, faccio lo XOR con la psw ed ottengo MD5 e quindi il keystream.
Ora se un utente arriva ed il keystream si ripete ottengo la password a gratis.

9.3 Lezione da RADIUS

Whitebox pentesting: alcuni siti usano nell'URL uno SHA256(emailuser, rand()), se provo a loggarmi, faccio brute force per capire qual'è il valore rand() usato: devo creare 2^{32} hash (se rand ha questa periodicità), con 66M hash/sec, 1 min e ho enumerato tutto i possibili valori, ora so che se entra un altro utente dopo di me, posso usare il mio dizionario per prendere il valore successivo.
Cosa ho imparato da RADIUS:

- Do-it-all-in-one non ripaga: un protocollo applicativo non dovrebbe includere sicurezza.
  Come rendo scuro un sistema? Sviluppo un protocollo apposito, come ad esempio TLS, e lo uso per rendere sicuro un protocollo non sicuro.
- AAA protocol non dovrebbe implementare un meccanismo proprio, inoltre non includere algoritmi nel protocollo.

Attualmente: DIAMETER per migliorare RADIUS.

9.4 AAA evolution: beyond RADIUS

Quando parto da una soluzione, meglio cambiare poco.
RADIUS deployato anni fa, oggi RADIUS è standard de facto per AAA, spesso anche usato in Wi-FI, supporto universale per i device vendors.
Buon protocollo, ma con limitazioni funzionali:

- scalability: quando fu deployato c'era pochi utenti, ma ora sono molti. UDP è unreliable, potrei avere problemi di loss
- diversità nelle tecnologie di accesso: prima dial up, ora Wi-Fi, 3G,4G etc..., devo supportare tutte: type|len|value era non sufficiente, 1 byte di type troppo poco.
  Lista di possibili estensioni: più di 256 combinazioni, servono più byte di type.
- interoperabilità: issue importante, ho un server central, ma non è realmente centralizzato (solo logicamente centralizzato), ho delle repliche ed è distribuito.
  Tutti i server considerati proprietari, quindi difficile avere interoperabilità.

Nota di scalabilità: mando RADIUS request e RADIUS accept una volta per connessione, quindi traffico è irrilevante per la scalabilità. esempio: ho NAS a 48 porte, ogni 20 minuti ho in media una nuova combinazione: $\frac{1}{20}\ minuti^{-1}$ ma $\cdot\ 48 = 2$ call/minuto. Ma se numero di NAS aumenta, tipo a 10000: 400 request/secondo. Dopo access request ho anche accounting request e delivery $\Rightarrow$ traffic può arrivare a diversi Mbps, quindi se scalo può diventare difficile da

gestire, potrei avere problemi di packet loss.
Quando dimensiono un sistema, di solito uso average load, ma non si considerano casi speciali: esempio, ho un crash e il device si reboota. Tutti i device rebootati mandano peek traffic: posso avere molta perdita, RADIUS non scala bene per colpa di UDP, ora serve reliability e quindi TCP o meglio.

9.5 IETF evolution

- Diameter: iniziato nel 1998, ora completato. Attività mosse in DiME(Diameter, Mainteinence, and Extensions WG).
  AP a casa: PPPoE/PPPoA: protocolli per patchare la possibilità di far girare PPP su ethernet o ATM, doveva durare poco, ma attualmente alcuni lo usano ancora.
- RADext: path a RADIUS, usato fino a che Diameter fosse diventato mainstream.

RADIUS: molto lavoro già fatto, pesanemente integrato, standard de facto.
Diameter: protocollo nuovo, più potente e scelta perfetta per nuovi scenari.
Li tengo entrambi: lavoro duplicato ma è conveniente a livello di business, se qualcosa va male in Diameter ho backup che è RADIUS.

9.5.1 DIAMETER

Simile ad """un object-oriented "protocol design" """ (non dirlo alle persone), ho classe base da cui derivo classe derivata. Primo protocollo inventato come OO: DIAMETER non è un AA protocol, ma un protocollo di messaging/signaling generico a lvl applicativo.Definisco il DIAMETER base protocol: ho le primitive per supportare messaging/signaling transport.
Definisco il protocollo per trasportare i messaggi, lo faccio in un altra classe base che è AAA Transport profile(SCTP, TCP-based), deve essere reliable.
Ora derivo le specializzazioni: creo una applicazione DIAMETER differente per ogni uso necessario:

- DIAMETER mobile IPv4 app: per muovere IP
- DIAMETER NAS app: questo è per il purpose di RADIUS.
- DIAMETER credit control app
- DIAMETER EAP app
- DIAMETER SIP app

Nella base: tecniche per keep alive server, load balance etc.., eredito le proprietà e specializzo per lo specifico porpuse dell'applicazione.

9.5.2 DIAMETER improvements

SCTP: perché TCP può non essere buono.
esempio: ho un NAS che deve parlare col server AAA. Quando arriva connessione, devo settare comunicazione, NAS manda request al server. La voglio reliable: soluzione base è setuppare TPC connection per ogni connessione: devo fare il 3-way handshake, mando il pacchetto e poi aspetto ack e mando il FIN. Tutto st'accrocco per un singolo pacchetto.
Non faccio TCP conn per ogni connessione. Uso una singola connesisone TCP per gestire tutti pacchetti: implemento multithreaded server: ho due thread, uno di questi si blocca. Vorrei poter gestire il secondo pacchetto, ma TCP fa consegna ordinata, quindi non posso creare gap nel protocollo: TCP mi da tutto in ordine, è uno dei goal. Ho un flow multiplo embeddato in una singola connessione TCP e quindi in un singolo flow.
Vorrei una connessione reliable che porta stream differenti, e vorrei un protocollo che garantisce che tutti i pacchetti nello stream siano letti nel giusto ordine, ma non di avere ordine fra gli stream: se il primo stream si blocca, vorrei bypassarlo e leggere il secondo. Effetto Head of the line blocking: anche se ho uno switch ad alta capacità, l'effetto impatta sulle performance.
Secondo problema di TCP: ho un NAS, per reliability ho una interfaccia ethernet, ma posso averne una di backup, ad esempio di backup (in altra tecnologia) così da garantire continuità. Ma l'IP address delle due connessioni è diverso e TCP socket usa la 4-pla: quindi se link fallisce devo inizializzare una nuova connessione (MPTCP lo risolve), vorrei supportare multi-homing: manage più IP address.
SCTP (Stream Control Transport Protocol) da queste due garanzie, protocollo migliore per canale di signaling dove trasmetto più flussi di dati.
storiella: perché se funziona così bene uso ancora TCP: chicken/egg problem. Standardizzazione bloccata dopo gli anni 2000, ad esempio anche IPv6. Problema dell'Internet Ossification: 1980/1990, con design spirit di Inernet che era End-to-end principle: nella rete telefonica originale, intelligenza nei device centrali, edge stupidi, in Internet la maggior parte dell'intelligenza ai bordi.
1995-1998-2000: web, avvento di device più intelligente, NAT primo device necessario per far fronte al lack di device alla rete, ma poi firewall, media converter ed altra roba messa sopra. Tutta una serie di middle boxes. Anche device come TCP accelerators, performance enanchements, etc... "intelligent devices". Arriva un nuovo protocollo: SCTP, comincio a connettere siti distanti, ma siccome traffico gira su questi device che lo reputano non noto, viene bloccato.
Servono middle boxes per supportarlo, ma i produttori lo fanno solo se l'evidenza mostra che è usato, ma come cazzo ti mostro che è usato se mi blocchi il traffico.
Ora software networking: middleboxes diventano software e sono controllabili, 5G è rete softwarizzata.

- Reliable transport: uso SCTP, senno TCP se non posso
- Standardizzazione in caso di errore: se server fallisce, come migrare verso

altro server. DIAMETER: standard per scoprire queste situazioni:

  - duplicate detection
  - controllo di ritrasmissioni a livello applicativo
  - fallimento di peer. DIAMETER è protcol p2p, server può startare comunicazione esplicitamente con NAS.

- pacchetti PING-like per testare se il device è attivo o no.
- Estensione dei limiti funzionali: header di RADIUS era corto, quello di DIAMETER è più complesso:
  - length di 3 byte
  - 3 byte comando ma anche ID per la specifica applicazione.
    Id del pacchetto serve per matchare request-response, lo scenario nel mondo reale non è solo point-to-point: ho multi-hop, ogni pacchetto averà un ID specifico. Non so se voglio matchare comunicazione globale o locale, quindi DIAMETER introduce due identificatori:
    * Hop-by-hop ID
    * End-to-end ID
  - altri flag: NAS può rispondere o far partire la comunicazione, sono in p2p: devo identificare se pacchetto è request o response, uso flag R, flag P sta per proxable e permette di specificare se il pacchetto può essere modificato da un proxy, flag E: messaggio di errore, flag T: messaggio potenzialmente ritrasmesso. esempio:
    mando un pacchetto, non ricevo answare e retx. Ricevo risposta: se server era bloccato temporaneamente, potrebbe rispondere di nuovo: uso T flag, così da darti avvertimento.
  - AVPs: i vecchi T|L|V triplets, ora chiamati attribute,value,pairs. Codice , lunghezza e attributo ma anche altro: metto vendor ID che dice che il linguaggio non è di DIAMETER, ma è customizzato.4 byte di AVP code, perché uno era troppo poco.
    Flags:
    * V: vendor specific
    * M: sono NAS e supporto DIAMETER v4.2.1, server DIAMETER v3.9.8, NAS vuole usare un attributo della nuova versione, che server non ha. Ricevo packet, con attributo che non comprendo: se l'attributo è importante, non posso skipparlo. Conviene droppare packet e dire al NAS di non aver capito. M serve per dire di rimandare indietro, perché le info non comprese sono mandatory. Risolvo interoperabilità.
    * P: se c'è encryption o no
  - ho il campo dati

Mangement di intermediate entities: posso usare RADIUS agent per mandare relayed message,ma non c'era supporto al romaning.
Non devo solo fare roaming data, ma anche routing: se mi collego ad un peer distante, quello deve fare route al server del mio paese. 3 cose strandardizzate:

- Nessuno agent intermedio
- Relay agent: sono a Roma, ma vengo dall'univeristà di Parigi, RADIUS server di Roma riceve la request, relay agent guarda al realm, ovvero il dominio di registrazione e nella sua routing table sa di dover mandare la richiesta al server RADIUS di Parigi.
- Proxy agent: simile al relay, ma assumo che può modificare il messaggio: se ho un messaggio con TAG integrità, se uso proxy e modifica ⇒ ho rotto tutto, è un MITM attack (proxy non ha la chiave per modificare il messaggio).

Eduroam: sistema che permette di roammare lungo le università confederate con eduroam e non richiede di avere credenziali specifiche. Cosa fa un utente che sta a Tor Vergata e vuole accedere, ma è di Malta: server parsa l'address e mi manda a Malta.
M se le confederazioni sono molte: che succede se il server di Malta è va giù e viene sostituito con nuovo server che ha cambiato ip? Deve comunicarlo a tutti gli altri, anche se aggiungo un server. C'è management nightmare: se uso relay agents o proxy agents c'è problema: le routing table sono embeddate, soluzione: centralized controller che tiene le routing tables. Tizio di Malta entra da Tor Vergata, va a server di Tor Vergata e server prima di inoltrare richiesta, chiede l'ip di Malta al centralized server: il dato rimane nel RADIUS server di Roma, ma il controllo è demandato al controller,posso usare trick di caching. Separazione fra controllo e dati ⇒ redirect agent: gestisce solo le routing table, ora le routing table non sono embeddate nell relay agent, quindi ho le due operazioni separate.
Questo rende ad esempio possibile number portability

10 Transport Layer Security (secure socket layer)

Analisi approfondita di TLS(/SSL) (il più famoso insieme a , SSH ed IPsec).
Disegnato per sicurezza di altri protocolli, ma c'erano problemi anche qui.2 obbiettivi: analisi dedicata di TLS nei dettagli, capire come fare design di un protocollo di sicurezza long-to-live.

10.1 Introduzione a TLS

Background storico di SSL/TLS:

- 1993, esplosione del web: Mozilla rilascia il primo browser e web diventa servizio reale. Subito dopo ciò, si ci rende conto che la sicurezza poteva diventare un problema cruciale.

- 1995: SSL v2 integrato in netscape 1.1, ma fu rotto quasi subito dopo la release.
- Capiti gli errori di SSL v2, c'è SSL v3. Approccio molto ben fatto in principio che è attulamente la base della versione attuale di TLS (oggi SSL v3.4 -¿ TLS v 1.3). HTTPS = SSL = TLS: SSL era il nome commerciale originale, era proprietario, che fu poi standardizzato da IETF e il nome fu cambiato in TLS, in modo particolare TLS v1.0 = TLS v3.1.
- 3 grandi momenti:
  - TLS v1.1: 2006, problema serio, perché TLS era stato disegnato pensando al web security, ma così stai facendo un'assunzione implicita sul protocollo di trasporto che usi ovvero TCP. Viene fuori che TLS usa le assunzioni di trasporto reliable, quindi se messo su protocollo unreliable non funziona più.
  - DTLS: standardizzato in parallelo a TLS nel 2006, versione di TLS adattata per girare un un transport protocol non reliable: preso TLS con pro e contro e modificato un minimo per farlo girare su un protocollo unreliable.
  - TLS v1.2: la versione usata oggi,anche se ce n'è una nuova. Corretto errore originale di TLS: protocolli vs algoritmi, il protocollo non dovrebbe contenere nessun crypto algorithm hardcoded. Se l'algoritmo viene rotto ⇒ il protocollo è rotto. Devi disaccoppiare per avere un long-time-live protocol.
    Nella parte pseudorandom del protocollo si dipendeva da MD5/SHA-1 (rotti dal 205 in poi). TLS v1.2 disaccoppia e supporta algoritmi per authenticated encryption.
- TLS v1.3: modifiche importanti, solo ciphers AEAD accettati, primo protocollo della famiglia TLS che garantisce la perfect forward secrecy.

10.2 SSL/TLS: layered overview

I due protocolli principali in newtowking runnanno a livelli diversi: IPsec garantisce sicurezza a livello 3 e runna sopra IP, quindi prima del layer trasporto e protegge anche il protocollo IP. Con IP sec ho anche integrity protection per pacchetti IP. Non ho nozione dello specifico layer di trasporto, sono il payload del pacchetto IPsec.
Mentre TLS ha obbiettivi diversi: nato per proteggere il servizio web, idea era prendi HTTP, fallo girare su un protocollo di sicurezza che era intermedio tra lvl 5 e lvl 4: TLS o DTLS. TLS quindi gira sopra il protocollo di trasporto ma non protegge il protocollo di trasporto. TCP rimane non protetto: mentre IP può garantire integrità del pacchetto IP (se ben configurato), TLS non lo fa: il pacchetto TCP può essere modificato. Un attacker può modificare la parte del TCP header, mentre la parte in cui c'è confidenzialità ed integrità è il messaggio HTTP (che è protetto da TLS).

Quello che TLS fa esattamente è proteggere esattamente il payload di TLS, ma non il resto. esempio:
VPN spesso create con IPsec, ma se uso open VPN:
ho il mio indirizzo IP, uso TCP/UDP ed uso TLS, poi di nuovo IP TCP applicativo. Tunneling: l'intera pila poggia su una pipe virtuale.
TLS esempio perfetto di protocollo di livello di sessione (pila OSI).
TLS non è necessariamente limitato al layer di trasporto, usato anche per altri motivi, anche per esempio EAP-TLS: autenticazione basata su TLS e protezione d'integrità su EAP v1.2. EAP-TTLS: creo tunnel su TLS e dentro scambio le credenziali, mentre in AEP-TLS uso TLS per scambiare certificati.

10.2.1 Application support

Socket per HTTP: creo connessione in cui specifico Ip addr, port number. N° porta è l'identificatore del servizio che lancio sulla mia macchina. (HTTPd su porta 80).
Server avere un approccio per livelli, dove ogni livello vede solo quello sopra e quello sotto e non più di uno:
vorrei usare HTTPS, potrei aprire la porta 80, ma ora potrei usare TLS e specificare che TLS usi la porta 123. Approccio corretto per fare incapsulamento sarebbe: TCP specifica che nel pacchetto ha un pacchetto TCP, dentro TLS specifico nell'header che l'application number è 80. TCP $->$ TLS $->$ HTTP. non fu fatto per ragioni storiche: nel 1993 nessuno pensò di usare TLS al di fuori del web. Approccio: ho HTTTP, se voglio usarlo uso porta 80, se invece voglio usarlo tramite TLS usa la porta 443, c'era un numero di porta dedicato. Perché una brutta idea: se uso per un servizio differente? TLS non ha un numero di porta specifico,se voglio usare ad esempio POP3, che usa porta 110 direttamente su TCP ma su TLS non posso usare la stessa: ora ne devo standardizzare una nuova; porta 995 che è SPOP3. Devo standardizzare una nuova porta ogni volta che voglio supportare un nuovo protocollo di livello 5: Duplication of port, non secure vs secure.

10.2.2 Confronto con IPsec

Tutto più clean: ho il classico header IP, ho un field di protocol che dice cosa c'è nel pacchetto: 6 per TCP, 71 per UDP, quindi IPsec standardizza 51 (ci sarà un header aggiuntivo per IPsec).Quindi, se ho IPsec connection e vedo pacchetto IP non so che protocollo sto usando: vedo protocol 51, l'avversario che guarda al mio traffico non sa che protocollo sto usando a lvl 4/5, meglio dal punto di vista della privacy. Ho un servizio detto traffic flow confidentiality: un avversario che guarda il flow di pacchetti non deve poter sapere cosa fai in termini di protocollo o applicazione sto usando (se è criptato); in TLS questa cosa non è vera: ho protezione sul payload ma non sull'header TCP da cui posso carpire le informazioni che mi servono.

10.3 Obbiettivi di TLS

Fa due cose allo stesso tempo

- Nel settare una connessione sicura (secure session in TLS) tra due end devo fare due cose: creare la connessione in se, faccio signal e setup della sessione sicura. Fatta dalla TLS handshake:
  - Quale algoritmo encryption uso, devo essere d'accordo con l'altro end. TLS non specifica o hardcoda un algoritmo specifico. per encryption
  - crypto keys che verranno usate: in TLS v1.2 cambiano in ogni connessione (asymmetric crypto). Qui i segreti sono sharati on the fly con tecniche avanzate.
  - Voglio essere sicuro che sto parlando con il server corretto: authentication.
- La seconda fase prevede il trasferimento dati: ho una chiave, ho definito il crypto algorithm, ho definito algoritmo di integrità, prendo TCP segments e li encrypto per trasferirli all'altro end.

Sarebbe meglio avere questi due due fasi implementate in due protocolli diversi: non dovrei fare le operazioni allo stesso tempo. Setto un'associazione sicura e la uso quando ne ho bisogno: questo viene fatto da IPsec, non proteggo traffico on demand ma è persistent. Approccio di TLS meno flessibile: in ogni connessione devo fare entrambe le fasi.
esempio: applicazione di TLS su IoT: voglio un protocollo come TLS ma il sensor device va a batterie. Se devi far girare un'istanza di TLS per ogni connessione, la batteria va giù. Split di TLS in due pezzi, separata la parte dell'handshake dalla parte dell'invio: creo sessione una volta e trasferisco i dati. In TLS v1.3 ha risolto il problema.

10.4 Protocol stack TLS

TLS gira su TCP/UDP. TLS wrappa i dati in un TLS Record Protocol, formato per scambiare dati. Sopra TLS posso far girare qualsiasi protocollo applicativo TLS non lo sa e non gli interessa, lo sa TCP per via della porta usata), nel TLS RP avrò: dati applicativi, c'è handshake protocol (che usa la stessa struttura del TLS RP), Alert protocol e change Cipher protocol; anche protocolli per gestione errore.

10.5 TLS Record Protocol

TLS v1.3 cambia parecchio. Voglio capire come di fa il design di un protocollo, quindi capire bene gli errori fatti.

10.5.1 Record Protocol operation

Preso dallo standard TLS v1.0, e vale fino a TLS v1.2: application data, taglio in frammenti, comprimo per usare meno banda. Aggiungo integrità (MAC), encrypto e poi mando il pacchetto. 2 grossi errori: da un punto di vista del protocollo sembra tutto ok, ma dal punto di vista della sicurezza ci sono. Gli errori sono usciti fuori dopo, specialmente la compressione fu usata per attacco CRIME (prima compressione e poi encryption è deadly) e nel fatto di fare prima integrity e poi encryption: cambia l'ordine? Irrilevante dal punto di vista del protocollo, am l'ordine conta: problema scoperto nel 2002, fixato, rotto di nuovo poi di nuovo rotto e poi di nuovo rotto e ancora e ancora rotto e rotto e ROTTO: padding oracle attack. Alla fine, TLS rende impossibile fare MAC separato da encryption, ma solo AEAD.

10.6 Compression

Application data sono verbose: ASCII, XML, HTML etc... Quindi in TLS penso alla compressione dei dati. Devo farlo prima dell'encryption: perché non posso fare encryption prima di compressione? Entropia: qualcosa può essere compressa solo se l'entropia è minore di 1 bit. Un buon encryption scheme è pseudo-random string con la stessa entropia $\Rightarrow$ non ha senso comprimere dopo. Lossless compression: introdotta da SSLv2. Considerato in TLS v1.0 ma non specificato: unico algoritmo standardizzato era null compression method. 2004: supporto per la compressione in TLS, nei successivi anni la compressione comincia ad essere supportata da vari browser fino all'uscita del CRIME attack: combinazione di compressione ed encryption è deadly (aiuta a decriptare).
Possibile solo usare HMAC, l'hash function è scelta dall'utente. La chiave è simmetrica ma non pre-shared bensì generata dinamicamente.

10.7 Encryption

Prendo il blocco dati, li comprimo, aggiungo MAC ed ora lo encrypto. Posso usare sia stream cipher che block cipher.
Algoritmo negoziato durante l'handshake, l'algoritmo non può aumentare la taglia di più di 1024 byte (ma non succede quasi mai, i blocchi sono di qualche decina di byte).
Infine ho il plai text compresso, il MAC tag, encrypto tutto ed aggiungo header:

- Content type che informazioni ci sono: handshake messgage, application meassge o alert
- Major version: 3.1 per TLS
- Minor version: 3.1 for TLS
- Compression length: lunghezza della compressione.

Cosa manca? Reply attack? Integrità non garantisce da reply attack senza una nonce all'interno. HMAC è funzione del segreto e del message content, poi ho enrcyption e se uso encryption deterministica o l'ho disattivata (non è mandatory). Ma posso fare un reply attack, manca la nonce: può essere vulnerabile a reply attack.
Perché non c'è un sequence number? Perché è implicito: quando faccio partire una TLS connection e dico che questo è il pacchetto 0, girando su TCP sono sicuro che i pacchetti arriveranno in sequenza ⇒ non serve includere il n° sequenza.
Quando computo HMAC: prendo i dati, includo header di TLS ed un numero di sequenza, che non trasmetti: il mio receiver saprà qual'è perché il traffico passa per TCP.
Ma ora c'è un problema: TLS funziona solo se uso davvero TCP e quindi per UDP si romperebbe la sicurezza. Per questo in DTLS è stato necessario ristandardizzare l'header, aggiungendo 8 bytes di seq num.

10.8 More insights on encryption+authentication

Come combinare encryption e MAC.3 possibilità:

- TLS: MAC then ENCRYPT: prendo i dati in plaintext (compressi ma dal nostro punto di vista è paintext). Aggiungo il MAC computato sui dati e poi uso encryption su MAC+dati.
- IPsec: ENCRYPT then MAC: prendo i dati, li ecnrypta e poi computa il MAC sui dati encrypted.
- SSH: ENCRYPT and MAC: prende i dati e su un lato fa MAC sui dati ed encrypta solo i dati. Argomento fallace è perché criptare il MAC, che è già una trasformazione crypto.

Problema: quale delle costruzioni è la migliore, ovvero assumo che uso un encryption scheme semantically secure (IND-CPA) ed un MAC sicuro (unforgiable), quindi MAC perfetto e dovrei dimostrare che con questi combinati ho ancora le proprietà originali.
Perché la combinazione non è più semantically secure (no IND-CPA): ragiono su un esempio con SSH:
in un plaintext-ciphertext so che posso avere A o B. Do un pezzo di cipher e ti dico di scoprire quale lettera è. Ho la possibilità di scoprirlo con un coin-flip. Ora encrypto A = α ed aggiungo il MAC di A che è x12; poi encrypto B = β ed il suo mac y34.
Non so cosa c'è nel cipher, ma il MAC lo vedo: coin-flip diventa deterministico. Il MAC di A o di B è deterministico, quindi si ripeterà. SSH quindi rompe la semantic security.
La strada giusta è quella di IPsec, quella di TLS è sbagliata.
Padding oracle attacks: iniziano nel 2002 e finiscono nel 2016

10.9 Attacchi a TLS

10.9.1 Background su block ciphers

Differisce dallo stream cipher per quello che riguarda l'operazione di encryption. Prendo i dati e li spezzo in blocchi, applico una pseudorandom permutation che trasforma il blocco in ciphertext. Trasformazione deve essere reversibile: se $PT_1 \neq PT_2$ anche i cipher lo sono.
Ma lo stesso plaintext viene cifrato con allo stesso ciphertext, quindi devo anche avere un modo di combinare il plaintext.
Come non farlo: applico solo sa trasformazione (electronic code book, ECB) $\Rightarrow$ sbagliatissimo: non ho semantic security. Se si ripete il plaintext, si ripete anche il plaintext.
CBC encryption (cipher block chaining): se m[0] = m[2] allora se li cifro senza fare nulla ho lo stesso cyper text. Perché non mischiare i blocchi con altri dati: prendo $PT_1 \oplus IV_1$, $PT_2 \oplus IV_2$ etc... e trasferisco i CT con i rispettivi IV. Genero un random IV ad ogni valore, ma il problema è che renderebbe ciphertext il doppio (IV deve avere la stessa taglia del plaintext). Cipher block chaining: prende IV (32 bit in SHA-256), faccio XOR con il messaggio m[0] ed ora faccio PRP con cui produco il ciphertext.
A questo punto uso c[0] come inizializzazione del prossimo blocco.

10.9.2 CBC padding

Voglio fare encryption usando block cipher: se i dati sono di 8 byte, il campo dati + MAC non è detto che sia di taglia giusta (può non essere multiplo di 2). Quindi se uso CBC, TLS deve paddare i dati: aggiungo qualcosa per riempire il blocco, che poi dovrebbe essere rimosso. Idea di TLS: usa l'ultimo byte dice quanto è la taglia del pad, se è 0 vuol dire che non ce n'è pad. Inoltre, se uso ad esempio 1 byte: lunghezza sarà = 1 ed anche il byte in più sarà un 1. (se ne uso 10: metto 10 byte di pad + una lunghezza = 10 e tutti i byte avranno valore 10).
Anche se la lunghezza del blocco non ha bisogno di padding, ormai mi aspetto che l'ultimo byte sia la length, quindi devo aggiungere comunque i byte di paddin+len: PKCS specification per il padding, posso estendere il padding fino a 255 byte.
Quindi: ho dato è MAC, nell'ultimo byte metto la lunghezza del padding ed aggiungo il pad.
Proprietà: come fa un server a decriptare? Mando un dato + MAC + padding + length, encrypto e mando al server. Il server lo riceve e deve decryptare: se ad esempio usa CBC ed usa AES (16 byte) ed ho 48 byte (o comunque multipli okay)di lunghezza sono ok, altrimenti penso ci sia qualcosa di sbagliato, mando messaggio di errore fatal perché la decryption fallisce.
Se invece la lunghezza è ok decrypto e riottengo il pattern di partenza: ultimo byte mi dice quanti byte di padding ci sono. Se ricevo un pacchetto in cui i byte paddati non coincidono con il byte di length(es: length = 2 e bytes 7 ed 1), so che qualcosa è andata male, la decryption fallisce.Ora so che i byte rimanenti

sono MAC è dati e so quanti byte compongono i singoli campi e posso checkare il pacchetto: se non è ok mando un messaggio che dice che il MAC check è fallito (bad_record_mac).
Perfetto se stessi considerando solo di networking: se c'è un errore devo farlo sapere all'altro end. In security questo non si fa: questo meccanismo è la base di un attacco, posso decryptare il pacchetto usando solo questi error codes ⇒ padding oracle attack.

10.9.3 Padding oracle attack

Sfrutta le scelte sbagliate nel protocollo. Scoperto nel 2002, fa capire perché l'approccio del MAC then ECNRYPT è sbagliato. Abbiamo il padding, necessario quando si usa un block cipher, il blocco deve essere un multiplo del block size e spesso questo non avviene quindi paddo con dei bytes extra. Riservo sempre l'ultimo byte per la lunghezza del padding (quanti bytes extra ci sono).
In crypto quando qualcosa fallisce NON si spiega la ragione: l'attacker può usarlo per decriptare l'intero messaggio.
L'attacco: funziona se viene usato CBC di qualunque tipo (anche il migliore come AES-CBC che oggi è considerato sicuro).
Ricevo un messaggio in ciphertext: IV + c[0]....[n]. Il mio obiettivo è decriptare un singolo blocco, per esempio c[1]. Assumo che l'attacker può fare Chosen Cyphertext Attack: l'attacker può forgiare ogni ciphertext arbitrario e mandarlo al server e vedere la risposta. È un attacco molto realistico: se vedo una connessione e dei messaggi, dopo il msg n° 2 posso creare il msg n° 3 ed inviarlo. Quasi sempre il msg n° 3 che è inventato non sarà corretto, quindi la connessione si interromperà ma posso vedere la risposta.
Voglio decriptare c[1], mando un ciphertext arbitrario e mi aspetto decyption failed o Bad MAC. Ma cosa vuol dire bad MAC: attacker ha selezionato un cyphertext random, es 93142197 e questo è stato decriptato lato server e la decrypt è meaningless es 19123111 ma se ricevo bad_record_mac ho informazioni sul plaintext che ho inviato: la parte finale è 0, o 11 o 222 quindi so che gli ultimi bytes sono un padding corretto (se ricevessi un bad encryption non lo saprei).
Uso un oracolo, che mi dice se il padding è ok o sbagliato:

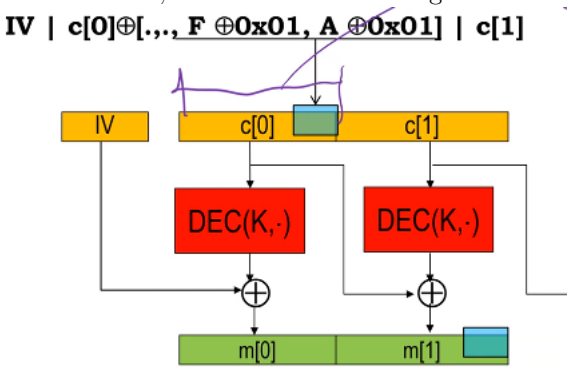
- Padding Ok è bad MAC
- padding wrong è decryption failed

In CBC prendo il plaintext, lo choppo in blocchi, uso IV col primo blocco m[0] e lo metto in XOR. Poi lo passo al PRP ed uso il risultato per m[1].
In decryption faccio l'opposto: ricevo IV, prendo c[0] applico PRP^{-1} e faccio XOR con IV ed ho m[0]. Poi prendo c[1], faccio decrypt e metto in XOR con c[0] ed ottengo m[1] e così via.
I bit di c[1] sono mischiati, quindi se cambio dei bit ho risultati impredicibili. Ma il fatto che uso c[0] nello XOR con c[1] senza passare per non linear transformation è la chiave per l'attacco.

Voglio scoprire un messaggio in plaintext: vedo un messaggio legittimo IV c[0] c[1]....
Levo la parte del messaggio che non mi interessa, faccio si che c[1] contenga l'ultimo byte del pacchetto e lo mando al server. Posso indovinare se l'ultima lettera è A?
Prendo c[0] $\oplus$ A $\oplus$ 0.Il messaggio va al server e farà i check:

- È di taglia giusta, perché ho tolto blocchi interi
- Posso decryptare? Sì
- Suppongo che il contenuto del messaggio fosse: Ciao I am Flavia, sto modificando l'ultimo byte facendo XOR con A e 0. Quindi l'ultimo byte del plaintext è 0 (quello del blocco affianco).
- La del server è bad record MAC: il messaggio è valido perché termina con 0, quindi lo rimuove e checka se la parte del messaggio è hashing corretto. Non lo è, però ho un'informazione e riguardo l'ultima lettera.

Per due lettere, il meccanismo è analogo:



Prendo messaggio originale, lo spezzo così che l'ultimo blocco è quello che attacco, faccio XOR del blocco prima tra l'ultimo byte, il byte che volgio testare ed il byte 0x00..0 così che se il guess è corretto il byte diventa 0 e ricevo bad MAC, altrimenti ricevo decrypt failed. È un test su una singola lettera nel plaintext.
Se lo ripeto più volte: ho indovinato l'ultima lettera, posso testare la penultima: guesso se termina con FA. Prendo c[1] $\oplus$ FA $\oplus$ 01 01.
Sta volta uso 01 01 quindi di nuovo avrò che il padding è ok se il guessing è ok.
Quanto è lungo l'attacco ad un intero blocco: meglio di un brute force attack, in brute force avrei 256^8 se avessi 8 byte di blocco, qui passo a 256x8 = 2^{11}.
Ma dopo il primo tentativo, la connessione si interrompe.
esercizio: ho un cipher f1 aa 11 04 —— 34 35 f1 20 —— 11 01 9c 01 —— ac c3 83 02 —— 65 61 fb 08 —— 91 11 5f 10. Voglio scoprire il 16° byte con padding oracle attack è 0x0f = 00001111.
Per prima cosa devo rimuovere la parte che non mi interessa: il byte che attaco deve essere l'ultimo. Per modificare il byte: ho 11 01 9c 00000001 —— ac c3

83 02 e gli ultimi sono cambiati da PRP^{-1}, quindi devo cambiare l'ultimo byte del blocco precedente così da avere effetto sul byte del blocco affianco.
Ora mi verrà che l'ultimo byte è 00000..0 e quindi potrò vedere il mio guess.
Quindi: se voglio scoprire un byte:

- Choppo il messaggio lasciando il blocco di cui voglio indovinare il byte alla fine
- Faccio XOR del ultimo byte del blocco precedente con la lettera che voglio indovinare e con 0x00.
- Quando verrà decriptato: se il byte è corretto, avrò che l'ultimo byte che sto cerando di indovinare è un 0 e quindi verrà visto come un padding. Verrà scartato ed il server cercherà di checkare l'integrità. Questo fallirà ed avrò bad MAC e quindi saprò ch ci ho preso. Se invece ricevo dab decryption, ho sbagliato il guess.

Se voglio indovinare più byte devo andare linearmente (0, 11, 222, 3333 etc...).
Come faccio a prevenire l'attacco: ho standardizzato due messaggi per due situazioni diverse. Correzione: restituisco una sola risposta, triviale (la maggior parte delle implementazioni corresse mandando sempre bad mac).
Se la decriptionva a buon fine, se check fallisce restituisce bad MAC che però è il vero bad MAC. Sono sicuro che attacker non può capirlo? Uso il tempo come indicazione per capire se il msg di errore è avvenuto a livello di encryption o di vero bad MAC. Side channels: problemi, come in questo caso per colpa del tempo.
LAN, quindi rete eth: la risposta può essere diversa per veri bad MAC o decryption failed. Mandando pochi messaggi è possibile discriminare quali dei due errori ho avuto.
Il programma sarebbe sequenziale, mentre un crypto programmer cercherebbe di fare entrambi i check in parallelo. (se faccio dei check e setto un flag di conseguenza e poi passo ad un compiler con flag -03 che però non capisce che che sto facendo programma per sicurezza).
Tutte le implementazioni corrette:

- TLS 1.2: valida il MAC anche in caso il padding fallisca
- Ma in che caso i dati vengono validati?Se messaggio è formattato bene, so quanto devo paddare, ma dopo decryption non so quanti dati devono essere validati. Se padding è di 2 bytes il msg finisce ad un certo punto, ma al variare del padding ho taglie di messaggi diverse. Decisioni complesse, quindi quanti dati valido? TLS 1.2 valida tutto, considera come max size msg, ovvero anche se padding fallisce considera msg — MAC e ultimo byte
- Kenny Patterson: HMAC, il tempo di computazione non è lineare, ma a scalini. Quando computo HMAC ogni blocco è computato con una f. di compressione. Posso misurare Δt tra i le varie lunghezze di blocchi? Attacco lucky thirteen: c'era ancora time channel

- POODLE: altro attacco, 2014
- 2015: altro subtle time channel
- 2016 attacco alla patch per fixare l'attacco lucky 13.

10.9.4 Lezioni

Problema è sempre quello: prima decryption e poi computazione MAC. Prima MAC e poi ENCRYPT protegge da questi attacchi: non posso più fare CCA, prima checko l'integrità e solo poi vado avanti. Ma se l'integrità non è verificata non ho modo di fare CCA; l'ordine delle operazioni conta.
Quando si ha a che fare con la crittografia bisogna stare attenti: non va in conflitto con security by obscurity, quello dice di usare open algorithm. Ma quando sono a runtime devo stare attento se quando differenzio una risposta, può esserci un oracolo che le differenzia e da delle informazioni all'attacker.
Non implementare crypto da se, attenzione ai side channel attacks.
Usa librerie cryto fatte da gente esperta: openSSL, LIBSODIUM, etc... (stesso vale per l'hardware).
L'attacco è pratico? Posso forgiare un cipher al server e dopo la riposta ho un errore fatale, che fa si che la connessione si rompa. Devo mandare 2048 messaggi, la prossima connessione partirà con una chiave nuova. L'attacco sembra non pratico, ma in qualche caso specifico può diventarlo. Telefono checka le e-mail, probabilmente ogni 5 min (perché si usa IMAP): setta connessione TLS, ed ogni volta la passoword e l'id sono nella stessa posizione. Sono attacker, conosco il formato di IMAP e voglio conoscere la password: so che sta nel blocco 3. Vedo il primo messaggio, provo con il primo messaggio, anche se fallisco dopo 5 min posso riprovare. L'informazione è strutturata sempre nella stessa maniera: posso fare più trial.
Dimostrato nel 2003 che era possibile intercettare e raggruppare le psw degli utenti tramite IMAP (usarono euristiche come dictionary atk etc..)
Quindi la vulnerabilità è estremamente pratica.
Cryptography Doom Principle (Moxie Marklinspike, crittographer che ha standardizzato la sicurezza di WA): se devi fare ogni operazione crittografica prima di verificare il MAC sul messaggio ricevuto, in qualche modo sei condannato.
TLS 1.3 standardizza AEAD, visto che non era possibile cambiare l'ordine delle operazioni (modifiche sw troppo importanti), non più MAC then ENCRYPT.

10.10 Block ciphers

L'obbiettivo è quello di generalizzare un substitution cipher: esempio sostituisco una lettera con un altra (vedi esempio de Giulio Cesare). Definisco un blocco: input è plaintext di taglia nota (in AES per esempio è 128 bit) e l'ouput è una stringa di altri 128 bit, diversa. Rimpiazzo dei 128 bit con altri 128 bit: ho 2^{128} possibile input, il rimpiazzo è guidato da un chiave segreta che è il tipo di sostituzione che vado a fare: k seleziona una delle possibile permutazioni.L'algoritmo di blocco (difficile da disegnare) dovrebbe implementare una

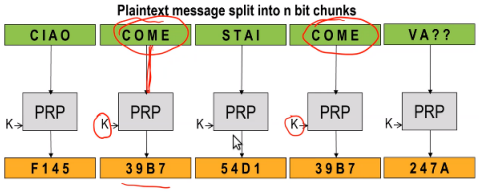
pseudo-random permutation o PRP, chiave dovrebbe selezionare una tra tutte le possibili permutazioni (in pratica, sceglie tra un insieme di queste)

10.10.1 PRP

S è l'insieme di tutti i possibili plaintext, se n = 3, la cardinalità di S è 8. Una permutazione è una biezione Π che associa ad ogni elemento di S un altro elemento di S. Voglio che la trasformazione sia reversibile.
Pseudo-random: il block cipher dovrebbe selezionare uniformemente una delle possibili permutazioni.Se ho 8 simboli, ho un totale di permutazioni=2^n!. A seconda del valore della chiave avrò una certa permutazione associata. La permutazione Π_k è associata alla chiave k.Quante permutazioni associate a quante chiavi: se ho 3 bit, $2^3! = 40320$ (posso avere anche la permutazione identica, ma nella pratica non si usa). Con 8 bit, ho 256 simboli differenti che si permutano in 256!: 8.58x$10^5$06. In AES n = 128 bit, numero di simboli è 2^{128}, n° permutazioni è 2^{128}! che è una roba non pensabile.Dovrei avere una chiave di 10^{40} bit mentre in AES sono di 128, 192 o 256. Se considero chiave di 256 chiave ho un numero totale di chiavi di 2^{256} che è il max numero di permutazioni che è molto molto minore del totale delle permutazioni (ricorda che ad ogni chiave è associata una specifica permutazione); probabilità di selezionare la permutazione random è ϵ. Considero quindi un subset dell'insieme delle PRP, ma siamo comunque ok (vedi ad esempio AES).

10.10.2 Problema 1-Plaintext più lungo della taglia del blocco

Ho capito che cos'è il PRP, mi fido che è ben fatto da crypto guys (se vedo alcuni mapping non posso sapere a cosa mappa un certo valore basandomi sugli altri, questo come nozione di sicurezza del PRP).
Plaintext più lungo della taglia del blocco, devo fare qualcosa: posso pensare di dividere il messaggio in chunks di taglia uguale alla taglia del PRP block (128 bit in AES ad esempio) e passare ogni blocco al PRP. Sbagliato: se m[1] ed m[3] sono lo stesso messaggio, il PRP fa si che il ciphertext si ripete, perché la chiave è la stessa



Perdo la semantic security, non IND-CPA secure.L'approccio è chiamato Electronic Code Book (ECB), e non va bene (big red flag).

10.10.3 Problema 2-Stesso plaintext

Ho visto il problema di ECB, ma se il messaggio è più corto? Ho ad esempio 8 lettere di messaggio ed il PRP usa blocchi di 8 byte, quindi uso un singolo

blocco e qui ECB potrebbe funzionare. Ma se lo encrypto di nuovo, riottengo lo stesso ciphertext.
Riuso l'idea dell'inizialitation vector: lo uso per ogni nuova encryption: prendo plaintext lungo quanto un singolo blocco, genero l'IV che deve essere di taglia uguale al plaintext. Li combino con XOR, ottengo sempre 8 byte di risaluto ed ora uso PRP indicizzata dalla chiave k ed ho il mio ciphertext.Posso trasmettere l'IV in chiaro con il plaintext, quindi c'è dell'overhead. A receive side: prendo cipher, faccio PRP^{-1}, faccio XOR con l'IV ed ottengo il messaggio; va tutto bene se la taglia del messaggio è $\leq$ della taglia del blocco.
L'IV non si ripete mai? Ma non basta, deve anche essere impredicibile (alla base del BEAST attack). Ovviamente, se riuso lo stesso IV ed il plaintext è lo stesso l'encryption è lo stesso, inoltre non deve essere predicibile: una nonce non deve essere impredicibile, basta che sia fresca. In questa specifica applicazione non è così.

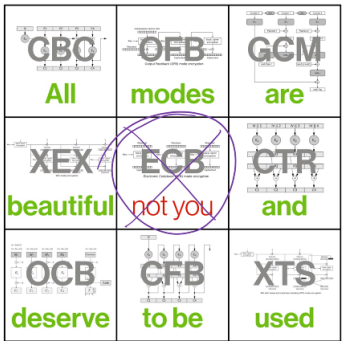
10.10.4 Modes of operation

Non usare mai ECB, usabile solo se :

- Messaggio è minore o uguale ad un blocco
- Messaggio non si ripeterà

Solo in queste condizioni strette si potrebbe usare (ma meglio non usarlo)
Per messaggi ripetuti: si genera un IV, random e della stessa taglia del blocco.
Per messaggi più lunghi: modes of operation: ho due ingredienti:

- Il blocco stesso, cambia il modo di implementazione a seconda dell'algoritmo
- Modo di operare, ho visto solo CBC ma ce ne sono altre. Questo permette di criptare testo di lunghezza arbitraria e mi permette di criptare senza ripetizioni del cipher ne momento in cui ho ripetizioni nel plaintext.



I più usati in pratica: CBC o CTR(Counter Mode, preferita dal prof a CBC)
NIST raccomanda, oltre queste 2, CFB e OFB.
Alcune più sofisticate, che combinano authentication ed encryption
Semantic security: prendo il plaintext, lo taglio in blocchi e genero un IV indipendente e truly random che associo ad ogni blocco, a questo punto combino

in XOR con questi IV e poi produco con il PRP il mio ciphertext. Siccome IV è random, non ho ripetizioni, ma ogni volta che mando il blocco devo spedire pure l'IV, quindi non è soluzione pratica; è il meglio che posso fare.

10.10.5 CBC

Modo più comune è usare CBC:

- Prende blocco di messaggio, aggiungo IV al primo messaggio e faccio XOR con m[0]
- Trusto che PRP è pseduorandom permutation e quindi che c[0] sia come un "random" IV per il blocco 2
- Prendo c[0] come IV per il blocco m[1], quindi lo uso per fare lo XOR e poi passo a PRP.

c[i] = ENC=PRP(K, c[i-1] $\oplus$ m[i]).Overhead è solo un blocco extra, se messaggio ha taglia di m blocchi, il cipher è di m+1 blocchi.
La fase di decryption procede al contrario: prendo IV, metto in XOR con PRP^{-1} di c[0] ed ottengo m[0] che userò in XOR col risultato del PRP^{-1} del c[i] successivo. Encryption consuma tempo perché non è parallelizzabile, mentre la decryption lo è: se voglio decryptare solo un blocco faccio accesso alla RAM e decrypto solo quello (se ho salvato il ciphertext lì).
È il modo più comune di fare block cipher, è sicuro se IV non è predicibile e non si ripete.
È lento per l'encryption ma almneo è veloce in deryption (appropiato per accesso ad encrypted file system o DB). Servono 2 circuiti diversi per encryption/decryption: le due direzioni sono diverse
Inoltre, il plaintext deve essere multiplo del block size: se non lo è, paddo (esiste standard per questo), è necessario anche in altri casi.

10.10.6 Altri modi: CFB e OFB

CFB: prendo un blocco, prendo IV e ne faccio XOR. Applico PRP ed ottengo il ciphertext. Sto prendendo plaintext e applico due trasformazioni che sembrano encryption scheme: nella parte dell'XOR sembra uno stream cipher con keystream noto. Quello che CFB fa è: criptare l'IV, fare XOR col blocco di plaintext ed ottenere il ciphertext. Trasformo il block cipher in qualcosa tipo uno stream cipher. Ho un pad keystream ed ho l'XOR classico dello strema cipher. Ora faccio CBC chaining, uso blocco c[0] a cui applico PRP e faccio XOR col blocco plaintext successivo.
OFB: principio è lo stesso, parto dall'IVe ci applico il PRP ma ora uso direttamente questo risultato. Lo prendo, faccio PRP e lo metto in XOR col plaintext, per il blocco 1 faccio come in CFB. Posso partire da IV ed applicare i vari PRP, sembra molto di più uno stream cipher: parto da un seme e genero i vari keystream per criptare i plaintexts. CBC/CFB non sono parallelizzabili, mentre OFB sì: posso precomputare tutti i keystream.

Decryption in CFB: non devo più invertire il PRP, prendo IV, lo encrypto con PRP e faccio XOR col blocco in ciphertext per ottenere il plaintext.
Lo stesso vale per OFB; in CFB posso fare decryption in parallelo. Perché non usarli: problema dello short cycle:
OFB: IV $\rightarrow$ PRP $\rightarrow$ PRP $\rightarrow$ PRP... esempio: blocco di 3 bit, permutazione è selezionata random, parto dal primo e comincio ad iterare: mi fermo prima di 8, periodicità di 5.
Non tutte le permutazioni sono le stesse: alcune chiavi k potrebbe portare a permutazioni che risulta in short cycle. Se ho un IV sfortunato la periodicità cala. Posso avere anche cicli più piccoli, come 3.
Per usare questi sistemi serve anche conoscere le reali proprietà delle permutazioni, devo progettare AES per non avere short cycle, entrare nei dettagli etc... quindi piango.
Problema di CBC, CFB ed OFB, che in un modo o nell'altro fanno chaining dei blocchi: non ho garanzie che non finirò in uno short cycle a meno di aprire la scatola nera dell'algoritmo di PRP.
Come caso degenere, esempio: se ho 3 blocchi 011 011 011 ed uso CBC con IV 010 ottengo 3 ciphertext identici, quindi male.
Anche nel caso dell'hash chian(OTP) ho questo problema, per questo motivo in crypto si odia il chaining.

10.10.7 CTR

Counter mode encryption, molto semplice:

- Prendo un contatore, nonce completamente predicibile. Lo incremento per ogni nuovo blocco
- Faccio il PRP del counter (il counter deve avere la stessa taglia del blocco usato nel PRP). Ottengo i keystream differenti per costruzione del PRP, che è una biezione (non è più un hash) e se è fatto bene il keystream è scelto random fra le $2^{2^{135}}$.
- Periodicità: periodicità del counter, se vai da 0 a 2^{128} ho un PRNG perfetto che non si ripeterà, quindi non ho short cycles
- Faccio XOR del blocco m[0] con counter ctr ed ottengo c[0], stessa cosa per m[1] $\oplus$ ctr+1 = c[1]etc... Non c'è chaining, ogni blocco è indipendente ed ho chiavi indipendenti, che sono generate a partire da un contatore.
- Se conosco il counter e l'algoritmo, posso parallelizzare: se voglio blocco 200, prendo ctr = 200, uso PRP e computo c[200]. Stesso vale per decryption: voglio m[200], faccio PRP[200] $\oplus$ c[200] = m[200]

Non ho short cycles, incredibilmente efficiente in hardware perché parallelizzabile.
Iniziamento non molto famoso, ovviamente se counter si ripete $\rightarrow$ gameover, anche se lo suo per lo stesso messaggio: deve essere simile ad un IV.

AES-Crt: blocco è di 128 bit (AES), è stato standardizzato che se accetto che la taglia massima di encryption è 2^32 blocchi, ovvero 2^32x16 bytes = 500 GB, prendo gli ultimi 32 bit e li uso come counter ed uso gli altri 96 bit come IV: parto da 0 come crt ma l'IV sarà truly random. Vantaggi:

- Rende block cipher stream
- Combina vantaggi di CFB e OFB (molto efficiente per encryption di file system)
- implementazione efficiente hw e sw
- richiede implementazione solo dell'encryption block (PRP)
- Posso fare random access: se indicizzo blocco col contatore, posso convenientemente accedere (per esempio memoria)
- Se ben usato (IV truly random e non si ripete, usato per al più 2^{32} blocchi) è l'approccio più sicuro: è garantito che per ogni permutazione di AES-CTR non ho problemi di weak permutation, per costruzione non posso avere short cycles.

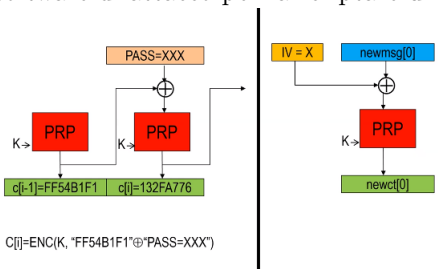
10.11 Vulnerabilità di IV predicibili

Per criptare due messaggi: i due IV devono essere diversi, ma questo non basta: l'IV deve anche essere non predicibile e questo sembra contro-intuitivo.
Suppongo di voler criptare m1|m2: prendo IV, choppo m1 ed m2 in blocchi, uso cipher block chaining così che l'ultimo blocco c di m1 sia usato come IV del primo blocco di m2. Uso IV per criptare m1, assumo che m2 usi l'ultimo ciphertext del messaggio m1. Sembra avere senso: perché la costruzione sopra in cui ho i due messaggi vicini è diversa da questa in cui il messaggio m2 è su una nuova riga? L'intuizione mi dice che se la prima costruzione è sicura (e lo è), allora anche la seconda lo è. Ma io ho scoperto che l'IV deve essere impredicibile: se uso la parte finale c[n] del messaggio 3, posso predire il prossimo IV: nella seconda costruzione sto violando la proprietà 2 di impredicibilità, lo vedo come ultimo ciphertext del messaggio trasmesso precedentemente.
Ho un messaggio legittimo, trasmesso da qualcuno. Posso solo vedere il ciphertext, ma ricevo un vantaggio: nel blocco m[i] del messaggio (assumo blocchi di 8 lettere) ho la stringa pass = XXX (non so cosa ci sia in XXX). Vantaggio 2: ??? non è sequenza arbitraria ma ha solo due possibilità: JOE o UGO. Basta per rompere il sistema? Lo sarebbe se fosse possibile fare dictonary-like attack: posso fare Chosen Plaintext Attack, 3° vantaggio è quindi di criptare un messaggio a scelta. Posso criptare PASS=JOE, guardo il ciphertext e vedere se combacia. Ma l'attacco non è possibile: se encryption scheme è semantically secure, ho un ciphertext diverso per lo stesso plaintext.
Se l'IV può essere predetto, posso rompere questa proprietà. Posso imparare, sapendo che l'IV è predicibile, selezionando un testo di mia scelta così da rivelare quale password è stata trasmessa nel messaggio precedente? Entro nel browser

e faccio criptare a TLS un plaintext di mia scelta: IV è predicibile, posso vedere ct[last] e so che viene usato come IV del prossimo messaggio, che è quello che l'attacker fa criptare: ho X predicibile, che è l'IV. Scelgo il messaggio: XOR è prima del PRP, se ho X $\oplus$ qualcosa come messaggio, prima del PRP posso vedere il qualcosa. Qualcosa = JOE$\oplus$UGO, quindi riapplicando l'XOR ho solo il qualcosa. Nel messaggio prima avevo PASS=XXX $\oplus$il cipher c[i-1]. Se metto nel testo PASS=JOE$\oplus$[c-1], mi rimane solamente il PASS=JOE se il guess era corretto.Quindi:

- Predico X
- Scrivo un messaggio che contiene X $\oplus$ c[i-1] del messaggio precedente $\oplus$ PSWGUESS
- Convinco l'implementazione a criptare il mio messaggio (verrà fatto X $\oplus$ X $\oplus$ c[i-1] $\oplus$ PSWGUESS = c[i-1] $\oplus$ PSWGUESS), se il c[0] risultante è uguale a c[i] (ovvero X), il guess è corretto. Altrimenti, la password è l'altra.

Effetto di overall è che se IV è predicibile posso fare trial and error attack.
Da un punto di vista del sistema: ho il browser web acceso e questo può tx un messaggio con TLS. Il messaggio ha la psw, per attaccare usando il browser uso software di attacco per far criptare un nuovo messaggio scelto da me.



10.11.1 Exploit in TLS-BEAST attack

Sembra un attacco teorico: se ad esempio la psw è 8 byte: 2^{64} try, quindi il CPA si può fare ma è idealizzato. Inoltre devo fare il CPA.
Il fatto che l'IV non dovesse essere predicibile era ben noto dal 1999 (Rogaway, IPsec), inoltre problema di standardizzazione in TLS 1.0: TCP trasmette in ordine, per evitare un IV fresco per ogni messaggio, l'idea è di usare il ciphertext dell'ultimo messaggio come IV del successivo, basandosi anche sul fatto che TCP lo permetteva.
In TLS 1.1+ fu corretto, aggiungendo un IV esplicito per ogni messaggio (mandatory in DTLS). Nel 2011 pochissimi usavano TLS 1.1
Beast attack: si credeva impredicibile, software issue: devo installare Trojan nel PC della vittima e fare injection di messaggi nel browser.C'erano nuove tecnologie come Websockets, HTML5 ed era possibile avere connessione aperta e catturare extra sources per fare injection. Altro motivo per l'impraticabilità era

la complessità: per decriptare un blocco di AES, quindi 128 bit di blocco, devo fare brute force di tutti i 2^{128} possibilità: non devo basarmi solo su psw, perché si usano spesso cookies (> 64 byte e molto entropici).2011: Attacco lineare nella dimensione del cookie (demo su youtube)
Come trasformare brute force attack in tempo lineare: per crackare un blocco dovrei enumerare tutti i possibili valori dei blocchi che sono 2128 tentativi. Ma è possibile fare injection di testo: quando mi connetto ad un server, mando un messaggio. Non conosco l'auth cookie, perché è nello storage sicuro del browser. Ma quello che posso fare è non solo fare injection di un nuovo messaggio, ma anche iniettare del testo di preambolo prima della connessione al server: creo un commento che aggiungo al messaggio (così che il server non lo parsi) e posso misurare la taglia del commento, posso muovere il limite da cui partire: se posso aggiungere testo per cui un carattere noto cada alla fine del blocco, devo fare 256 tentativi per crackarlo. Chosen Boundary attack: selezioni e cambi i limiti del blocco criptato.Ora è possibile attaccare: attacco la prima lettera, poi la seconda (lo forzi o aspetti il prossimo accesso). Complessità dell'attacco, se cookie è di N byte l'attacco è di N·256 tentativi, contro il 256^N.
Quindi, l'IV predicibile in CBC è exploitabile

10.12 CRIME attack

Compression leaks. Stessi autori del BEAST (orami avevano i trojan per muovere i limiti del blocco). TLS usa compression e poi encryption, anche se non posso decrpitare, la taglia della compressione rivela delle informazioni ma in teoria non sono usabili.
Compressione disabilitata dopo questo attacco.Problema non solo di TLS, ogni volta che c'è compressione e poi encryption può esserci un problema. C'era un paper del 2002 che spiegava come la compressione potesse rivelare informazioni sul plaintext.
Idea: posso comprimere e cripater due stringhe: AAAABC $\rightarrow$ 4ABC (se non trasmetto numeri), se non ci sono ripetizioni non posso fare nulla (es ABCDEF). Ora faccio encrypto: ad esempio con stream cipher vedo una stringa di 4 caratteri che non ha leak. Idea: plaintext injection nel BEAST attack, aggiungendo un preambolo per shiftare preambolo. C'è una password in plaintext, non la conosco. So che sarà compressa + criptata ad una taglia es di 6 byte. Ricordo che potevo aggiungere un preambolo: posso ad esempio mettere AAA o BBB o SSS come preambolo, ovvero una sequenza compressa. Guardo al risultato: se comprimo AAASHARON il risultato è 3ASHARON, BBBSHARON è 3BSHARON, ma SSSSHARON sarà 4SHARON. Primi due casi ho 8 byte, ma nel caso 3 ho 7 bytes $\rightarrow$ capisco la prima lettera. Se posso aggiungere un preambolo e forzare l'implementazione ad aggiungere il preambolo, allora posso rivelare una lettere e decriptarla.
Lo stesso problema può accadere se ho un DB, all'interno del cui ho dei dati privati, e che viene poi compresso e criptato. Se posso fare injection di dati nel DB, ho la stessa vulnerabilità; quindi non è solo un problema di TLS. Attacco CRIME funziona anche per block ciphers, cambiano i dettagli a seconda

dell'algoritmo di compressione. Possibilità di fare injection di testo, prima dei dati utenti: in BEAST era padding con commenti inutili, mentre ora è injection di testo scelto. Dettagli di uno specifico meccanismo, in questo caso DEFLATE, ma può essere applicato ad altri compression schemes.
DEFLATE: due tecniche, una bit oriented, un'altra è il Lempel Ziv algorithm: lavora a livello di byte, prende 3+ caratteri, fa un replacement: giuseppe bianchi and marco bianchini, primo passo del parser vede che "bianchi" si ripete (anche spazi si ripetono, quindi vanno compressi).Lascia la prima stringa inalterata, per l'altra aggiunge una coppia(-18,7): -17 dice di andare indietro di 18 caratteri (pointer) e il secondo numero dice quanti byte prendere (in realtà è (-17,8) contando gli spazi). Risultato è: giuseppe bianchi and marco (-18,7)ni.
Ho un testo utente legittimo, voglio indovinare la password:
GET /comment:twid=a HTTP1.1 Cookie: twid=flavia... Aggiungo un preambolo alla richiesta, che sia una parte di commento, in questo caso /comment:twid=a. Conosco format della richiesta di Twitter, quindi so che parte con twid= e cerco di indovinare la 6° lettera, ad esempio la a. Tutti i compression scheme usano una finestra per spostarsi, in quanto diventa difficile andare indietro, ad esempio di 2GB.
Una volta compresso: GT /commenti:twid=a HTTP/1.1 Cookie: (-24,5)flavia. Prende solo il preambolo twid=, ma posso ripetere finché non becco la lettera f, perché mi rendo che la taglia di byte da leggere diventa 6 invece di 5. Ora provo la lettera 2 e così via...
Attacco lineare all taglia del segreto, quindi molto pratico da effettuare. Anche se auth cookie è di 64B ho un O(64x256) nel caso peggiore, quindi attacco molto pericoloso.

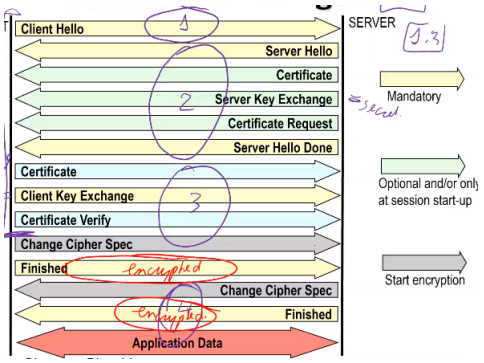
10.13 TLS Handshake Protocol

A partire da TLS v1.2, in TLS v1.3 differisce. Quando si usa l'handshake: connessione ad un server. https://www.fineco.it, ogni votla che mi connetto parte una handshake iniziale che ha come obiettivi:

- Mutually authenticated, ma di solito è unilaterale: quando apro TLS connection la banca mi prova la usa autenticità e una volta che il tunnel TSL viene stabilito (encryption ed integrity) mando username+password. La banca non sa se sono autentico a meno, uso PAP all'interno di TLS. Se posso assegnare all'utente un certificato di sicurezza, posso usare la mutual authentication.
- Non c'è algoritmo di encryption specifico: protocollo è disaccoppiato dal algoritmo crittografico di sicurezza, quindi si negozia l'algoritmo che verrà usato. Ma può essere attaccata la negoziazione: se convinco client e server che si può usare solo RC4? Bisogna proteggere questa fase.
- Servono nonces, scambio delle random quantity
- Serve scambio dei segreti per computare i segreti. Serve quindi asymetric cryptography, non posso mandare in plaintext

Se mi collego, e poi mi ricollego di nuovo il processo ristarta. Ma nella connessione scambio molti messaggi col server, idea di TLS è che ogni connessione deve usare una chiave di encryption e di HMAC diverse anche se le connessioni sono su due server diversi. Questo permette di ridurre il riuso di chiave ed evitare crypto analisys. Ma per usare nuova chiave, l'asymmetric crypto e computazionalmente costosa: symmetric vs asymmetric è 10^4 più veloce. L'idea è che posso riusare del lavoro fatto nel primo handshake per farne uno abbreviato, quello che si fa nel mondo reale. Su altre connessioni TCP uso handshake più leggere, abbreviate: sesison resumption, si riusa parte del lavoro della prima connessione per computare chiavi differenti per la connessione.
Obiettivi dell'handshake:

- Negoziazione sicura dello shared secret, con asymmetric crypto
- Autenticazione opzionale, facendo autenticare sia client che server, in modo da essere robusti a MITM. Non mi proteggo da ARP poisoning, DNS spoofing etc..., ma TLS garantisce che l'atk non può vedere o modificare il contenuto dei messaggi: ho integrity protection e encryption.
  Ma se la banca non è autenticata, atk si finge la banca, prende il traffico lo modifica e lo manda a Fineco ma questo è protetto dall'autenticazione. Tecniche robuste contro attacchi classici e strong, ma se attacco è del governo manco per nulla.
- Negoziazione affidabile: attacker non deve poter fare danni nella fase di negoziazione. Se mi scambio gli algoritmi di encryption ed un atatcker convince entrambi gli host che si può usare un protocollo weak è finita. Va protetto



Tutti i messaggi precedenti alle frecce grige sono in chiaro, aggiungo header di 5 byte ai singoli messaggi e li passo a livello 4 a TCP.
Header TLS:

- Content type
- Major version
- Minor version

- Length

Poi c'è payload del messaggio.
esempio: mi collego ad una banca, prima di inserire in miei dati solo la banca si autentica a me, io mi autenticherò passando username e password. Scambio TLS v1:

- Primo messaggio è mandato dall'utente al sito della banca, che è il Client Hello. Incapsulato su TCP/IP, la parte di TLS:
  - v1.0 (SLL 0301)
  - length
  - handshake type
  - 32 byte di nonce, contiene sia timestamp che random bytes. Ora deprecato il timestamp, non è autenticato quindi non è detto che sia un timestamp vero, quindi ora sono 32 byte du random e non più 28+4.
  - (Session id lenght, session id): può servire se voglio riusare una sessione precedente.
  - Parte della negoziazione: cipher suites e compression): in TLS, la prima cosa da fare è condividere il segreto, si fa con asymmetric crypto, anche detta public key cryptography. Devo scegliere l'algoritmo da usare: in TLS tutto va negoziato (no hardcode nel protocollo), possibilità di negoziare il public key algorithm: esempio TLS_RSA: uso di RSA come algoritmo asimmetrico. C'è anche una seconda parte: TLS_RSA_WITH_ algoritmo da usare per symmetric encryption ed integrity, quindi cosa userò quando comincia l'encryption dei dati. esempio: TLS_RSA_WITH_RC4_128_MD5.
    Oggi la lista di ciphers è estesa (è possibile specificare NULL per la parte dell'algoritmo di encryption e richiedere solo integrity, conferma del fatto che i due servizi sono diversi).
    La parte importante è che il protocollo non sia legato intrinsecamente al crypto algorithm.
  - Versione di Aprile 2012: negoziazione anche del compression algortihm (prima di CRIME), ora hardcoded NULL.

  Nel Client Hello do una lista di possibili algoritmi i supportati), ed il server ne sceglie una. Se il server è vecchio, può scegliere l'algoritmo peggiore (le opzioni sono messe in ordine crescente per livello di sicurezza). Negoziazione: client offre, server sceglie.

- Server Hello:
  - Handshake type

- versione del protocollo: anche la versione di TLS viene negoziata, anche questo è fondamentale. Per questo è presente la versione nel client: appariva in due parti, nel record protocol e nell'handshake. Nell'handshake c'è la proposta di quale versione usare, quindi il server può anche sceglierne una diversa se non supportata.
- Nonce del server, 32 byte(4 TS + 28 random).Server risponde 3 ore dopo? No, il timestamp probabilmente è considerato diversamente sui due sistemi, quindi 4 byte di TS erano uno spreco perché non c'era una time reference precisa.
- Ho un session ID ora
- Cipher suite: server risponde con un protocollo diverso da quelli che aveva il client come priorità

Ho appena visto la negoziazione della versione, downgrade attack (arma grande, difficile da fixare): client usa TLS v1.0 (SSL v3.1), server anche supporta TLS v1.0 ed assumo che la versione sia sicura.
Assumo che l'attacker non possa rompere TSL v1.0 ma possa rompere SSL v2.0
Attacker prende Client Hello, è in plaintext e senza integrity perché non ho un segreto shared, quindi non posso criptarlo, messaggio molto vulnerabile.
Vado nella parte del messaggio dove c'è a versione e cambio: cambio due byte, da 0301, metto 0200.
Server vede che versione è più bassa, ed accetta la connessione (oggi non è possibile scendere sotto TLS v1.0, poodle attack: downgrade di TLS + padding oracle). Ora attacker rigira la risposta al client, così che questo creda che il server abbia supporto alla versione di TLS/SSL più vecchia.
Agreement sulla versione di SSL v2.0, convinti che questa è l'unica versione usabile; è un problema fondamentale di tutte le negoziazioni.

10.13.1 Public key cryptography

Esempio di problemi risolti da asymmetric encryption: comunicazione tra l'app ed il server è essere criptata, ma il problema è dov'è la chiave. Se ho una SIM card, ho lì l'encryption key. Ma come risolvo problema del downaload di un applicazione: scarico e mando encrypted traffic, ma dove metto la chiave? Se metto nel codice, male: hacker wannabe 101 cerca pattern nel codice, faccio regex (della chiave) e guardo nel binary code dove il charset è ristretto a base64, quindi ho trovato la chiave. O predo la chiave da una comunicazione separata, ma come faccio: se devo chiederlo al server devo poterla trasferire.
Asymmetric cryptography: differenza con le simmetric key è che la chiave usata per criptare è diversa da quella usata per decriptare. Solitamente: prendo plaintext, applico una trasformazione che deve essere reversibile, ed ho il mio ciphertext. Ho visto stream e block cipher, ma si basano entrambi su una chiave preshared.
1970: schema dove

- La chave usata per encryption è diversa da quella per decrypt.

- Impossibile derivare una chiave dall'altra: se ad esempio conosci quella per encrypt non puoi trovare quella usata per decriptare

Se ho questo schema: user cripta i dati con una chiave, trasferisce ma la destinazione usa una chiave differente.
Problema risolto nel 1977 Rivest, Shamir, Adleman, RSA.
Le chiavi devono poter essere linkate, siccome sono asimmetriche e conosco K_{ENC}, K_{DEC} è nascosta, quindi come corollario posso avere K_{ENC} pubblica.
Come faccio quindi a risolvere il problema di sopra: scarico l'applicazione, che contiene anche K_{ENC}. Tutti vedranno K_{ENC}, è in plaintext. L'utente vede K_{ENC}, tutti lo vedono quindi chiunque può criptare qualcosa: ma nessuno vede la chiave K_{DEC}. Quindi, se uso la K_{ENC} per criptare i dati da mandare la server, nessuno potrà decriptarli.
Public key = K_{ENC}, private key = K_{DEC} (conosciuta solo da 1).
Perché continuo ad usare symmetric key:

- Risolvono due problemi diversi, non posso dire che una è meglio dell'altra
- entrambe possono essere sicuri o non sicuri
- Asymmetric è più flessibile, ma servono protocolli più complessi.
- (Algoritmi noti sono rotti dal quantum computing, symmetric no).
- Asymmetric è da 3-5 OOM (order of magnitude) più computazionale complessa.

Nessuno usa asymmetric encryption per trasferire dati, si fa questo: user ha la K_{ENC}, deve trasferire i dati, prima di fare questo genera una chiave k simmetrica, trasferisce $ENC_{K_{ENC}}(k)$. Solo il server può leggere, quindi ricava la chiave k simmetrica ed usa un algoritmo apposito (AES) per trasferire i dati.
Due possibili approccio fino a TLS1.2 per fare key management:

- Key transport (es RSA, ora non più usata):
  - server manda una key pubblica, che sarà nel certificate message (non può essere trasmessa in plaintext), client può anche salvarla se sa che la riuserà
  - Client genera un segreto random, che critpa usando la chiave pubblica del server e trasportato al server
  - Ora è possibile fare symmetric key encryption.
- Key agreement (DH algorithm), successo nel trasferire lo stesso segreto alle due side:
  - Tutti e due generano una chiave privata e pubblica, es Y, $g^Y modp$ ed X, $g^X modp$,se conosci $g^Y modp$ non puoi ricavare Y (vedi su la lezione sulle cripto hash)

- Client e server si mandando le chiavi pubbliche, l'attacker non riesce a ricavare facilmente X ed Y. Ma non è difficile per gli end: se ho g^X ed Y posso fare $(g^X)^Y$, quindi ho g^{XY} e posso ricavare le chiavi.
- Se l'attacker li moltiplica, ottiene g^{YX}??, No è la somma g^{Y+X}.

Quindi TLS può usare uno o l'altro modo, anche questo viene negoziato.
TLS handshake: Client manda Client Hello, server risponde con Server Hello e qui è stata negoziata la versione del protocollo TLS.
Ora con RSA per esempio: dopo il Client Hello, server manda una chiave pubblica certificata (attacker non può cambiarlo). Ora client applica key transport mechanism: genera segreto k shared e lo trasferisce al server criptato con K_ENC, non può essere modificato (o meglio lo assumo, rotto nel 2018). Server riceve il messaggio ed estrae il segreto shared. C'è altro trick: metto nel messaggio del client anche il codice della SSL version per prevenire il downgrade attack: se l'attacker l'ha modificato, io non mi fido e invece di essere d'accordo rimando la versione che avevo scelto inizialmente invece di quella accordata: ricordo di nuovo al server che potevo usare una versione più recente di SSL, ma lui ha detto di usare una versione più bassa. 2 byte di overhead. Ora l'attacker non può modificare i messaggi: né quello con la chiave pubblica né quello con la chiave shared dal client per il server. Quindi, il server si accorge che qualcosa è andato storto: mi rendo conto che il client mi ha rimandato la vecchia versione proposta e non quella accordata, quindi stoppo la connessione. Metodo fondamentale per risolvere downgarde atttack, nel momento in cui da un certo punto in poi la cripto è up: da quando è up, ripeto quello che ho negoziato. In un protocollo non posso essere sicuro di quello che accordo in plaintext.
Ma riguardo cipher attack? Attacker potrebbe convincermi ad usare altro protocollo di encryption, etc... Sto proteggendo solo la versione, inoltre cosa cambia tra i dure approcci: in DH non posso trasferire informazioni nei messaggi, ho delle quantità fisse, non è un public key crypto system, usa asymmetric crypto ma non è un crypto system così com'è: non posso trasferire qualcosa, come ad esempio la versione di TLS.

10.14 Asymmetric cryptography

Nell'encryption asimmetrica: prendo plaintext, uso chiave chiamata encryption key (algoritmo di derivazione della chiave noto), ottengo ciphertext e mando alla destinazione. Qui si una una chiave per decriptare che è diversa da quella usata per l'encryption, sono ovviamente collegate l'un l'altra ma non si può derivare una conoscendo l'altra (a meno di conoscere altri dettagli). Spesso K_{ENC} = public key e K_{DEC} = private key: chiunque può criptare ma una sola persona può decriptare.
HTTPS/TLS:

- nella fase di handshake, viene mandata una segreto shared.
- Nella seconda fase si usa key derivation functions per derivare dal segreto shared la chiave di encyption e di integrity.

- Refresh della symmetric encryption e message authentication usando sempre lo stesso segreto della prima fase (nel caso di nuova sessione?).

Hybrid encyption, spesso applicata. non voglio mettere su una connessione TLS, ma voglio fare encryption di un dato, esempio un e-mail ed uso una chiave pubblica, ad esempio quella dell'utente a cui voglio inviarla. Ma il messaggio è lungo:

- genero una chiave K simmetrica, random number
- Uso un cipher ordinario, come AES, ed encrypto messaggio usando la chiave K ed AES $\rightarrow$ symmetric encryption.
- Prendo k e la cripto con asymmetric cipher, e lo mando col messaggio. Mando un messaggio in cui nell'header ho asymmetric encryption della chiave, che è la chiave simmetrica usata per fare enctyption, più il campo dati. Sfrutto la velocità e scalabilità dell'asymmetric encryption.

10.14.1 PubKey crypto

Encryption e decryption sono una l'inverso dell'altra: DEC(ENC(M)) = M, quindi posso fare in questo ordine: public key encryption, un crypto system in cui sto criptando i dati in modo che tutti possano criptarli ma sono uno possa decriptarli. Assumo che l'operazione sia commutativa: ENC(DEC(M)) = M, ha senso dal punto di vista algoritmico (ma non semantico). Ha senso per fare la digital signature, è la duale del public key enrcyption: nel caso della digital signature

- Prendo la mia chiave privata, prendo un messaggio M ed applico $D_A(M)$, posso applicarla solo io perché solo io ho la chiave. Chi può invertirla? Tutti, quindi se trasmetto M, $D_A(M)$: chiunque può vedere il messaggio, l'extra information TAG (AUTH) e quindi se applico al TAG la trasformazione inversa, ovvero lo encrypto posso verificare se ottengo il messaggio originale o altro $\rightarrow$ creo integrity ma con asymmetric crypto.

Posso quindi creare due applicazioni diverse: usa è per l'encryption di dati, una per la digital signature. Devo trasmettere un messaggio: applico asymmetric crypto del primo caso. Applico una hash function crypto, comprimo ed ottengo digest e nessuno può ottenere lo stesso hash con un messaggio diverso. Quindi quello che faccio è la cosa seguente: ho messaggio compresso, trasformo usando l'operazione di decryption (che usa la chiave segreta), quindi trasmetto il messaggio più uno short tag. Per verificare se messaggio è vero o no: uso la public key per invertire l'encryption dell'hash computato prima. Quindi faccio hash del messaggio verifico se i due hash combaciano. Un attacker può solo scoprire cosa c'è nel tag invertendo con la chiave pubblica, ma non può in nessun modo ricavare un messaggio m' che mi generi lo stesso hash. L'hash del messaggio ha due obiettivi:

- Restringere il messaggio così da applicare trasformazioni su un singolo "blocco".
- Sicurezza: se non uso un hash, il sistema è vulnerabile, non solo per ottimizzare le perfomance, avrei un problema di malleability

Message integrity con authentication alla sorgente: in MAC, ho una sorgente, messaggio M ed il tag(K,M), ma se K è shared non posso autenticare la sorgente, non sono sicuro che l'abbia generato la sorgente, può averlo fatto anche la destinazione. Non c'è la non repudiation property (source authentication). Nella digital signature il concept è lo stesso, ma la chiave K usata nel TAG è privata ed è della sorgente.
Attacker può comunque prendere messaggio, sostituire la sua HASH + enc del messaggio e spacciarsi per la sorgente e rendere il messaggio valido.

10.14.2 Basic Algorithms

Pionieri: Diffie-Hellman key agreement, problema dell'asymmetric cryptography, vera soluzione 1977 da Riverst, Shamir, Adelman, RSA cryptosystem. Problema di usare l'approccio di DH in crypto systems fu risolto nel 1985 da El Gamal.
Problema generale: trovare un problema asimmetrico difficile in una direzione e facile nell'altra. esempio: hash function è un problema asimmetrico (da hash a digest facile, da digest ad hash è undefined).
Diffie ed Hellman trovarono problema: computazione del logaritmo discreto, ma non poterono costruire un crypto system su questo. RSA: non trovarono un modo di adattare il problema, ma trovarono altro problema:
ho p e q primi molto grandi, è facile fare il prodotto di p e q. Ma se ho n = p·q, è difficile trovare p e q, problema di fattorizzazione, approccio per trovarli è brute force (tento tutte le possibilità).
Ho un primo p ed un "numero" g (generator, poi scoprirò). Prendi x: $g^x mod p$ p è di 1024 bit, x anche può essere grande. Operazione è veloce o no? Se devo elevare $g^{132412394533242543}$, ma c'è trick per renderla più veloce. Devo computare $g^{1437} mod p$. Prendo l'esponente e lo traduco in forma binaria: $1437 = 10110011101_2$.Lo metto in colonna in ordine inverso (dal bit meno significativo al più significativo) e creo square e multiply. La prima linea è di inizializzazione, nel caso ci fosse 0, metterei 1 nel multiply (altrimenti metto g). Nelle seguenti linee: se ho un 1, nella multiply moltiplico il valore di Multiply della riga sopra per il valore della Square della riga corrente, mentre nella Square faccio una operazione, ovvero il quadrato della componente precedente.
Quante operazioni compio: 10 operazioni di Square + 6 Multiply, passo dalle 1436 operazioni iniziali a 16. Risultato generale: $log_2(numero)$ + le Multiply: $log_2(numero)$ nel caso peggiore, 0 nel caso migliore, avg: $\frac{log_2(numero)}{2}$ quindi in totale = $1.5 \cdot log_2(numero)$. Calo da complessità esponenziale a complessità logaritmica: lineare con la taglia in bit del numero. Dlog è complesso perché, dato un $y = 3^x mod 104729$, e chiedo di trovare un x tale per cui y = 33490. Se la funzione fosse monotona potrei applicare algoritmi molto efficienti per trovare

bit	Square	Multiply
1	g	g
0	g^2	g
1	g^4	g^5
1	g^8	g^13
1	g^16	g^29
0	g^32	g^29
0	g^64	g^29
1	g^128	g^157
1	g^256	g^413
0	g^512	g^413
1	g^1024	g^1437

il valore di x. Ma in questo caso non è così, la complessità rimane esponenziale. Quindi ho il problema che volevo trovare.
Diffie-Hellman, protocollo di key agreement, permette di settare tra client e server un segreto shared, non trasferendolo da una parte ad un'altra, bensì usando computazioni: asimmetrico nel modo in cui ricavo il segreto shared, scambio dei valori pubblici.

- Alice genera una quantità random, x. Bob genera y, random.
- Alice manda a Bob $g^x modp$, si computa facilmente. Bob manda $g^y modp$
- Alice prende $(g^y)^x modp$ ed ottiene k. Bob fa lo stesso, ed ottiene la stessa chiave k. Ho applicato di nuovo modular exponentiation, veloce.
- L'attacker ha visto lo scambio, ma non può computare la chiave perché deve invertire il dlog. Da g^x e g^y è difficile computare g^{xy}. Bob ed Alice hanno i "segreti" x ed y, quindi per loro è facile fare la computazione.

esempio: p = 29'996'224'275'833, g = 3 (sono parametri). x = 123456789, y = 234567890. Alice computa $g^x modp$, Bob $g^y modp$. Poi, alice farà $(g^y)^x modp$, mentre Bob farà $(g^x)^y modp$, ed avranno la stessa chiave K. In Diffie-Helmann: numeri di almeno 1024 bit.
La sicurezza dell'algoritmo si basa sul fatto che l'attacker deve per forza invertire uno dei due dlog: se conosco di più, ovvero x o y, allora posso riuscire a ricavare k: questa è la proprietà di asimmetria.
Limiti di DH:

- Non implementa un crypto system: risolve un problema, ora che ho la chiave K shared, posso usare AES-128_K(data), quindi ho risolto il problema pratico di trasferire i dati su un canale non sicuro. Ma non risolve la challenge originale: prendi un messaggio M, criptalo con una chiave K_{ENC} e decriptalo con K_{DEC}
- Non posso derivare facilmente una digital signature, non posso usare la chiave SK per la DS (non avrei la non repudiation property)

1977: RSA per risolvere il problema (ora non si usa più perché non ha implementazione efficiente su curve ellittiche).

10.14.3 RSA Algorithm

Algoritmo i Rivest, Shamir e Adelman; patented fino al 2000.
Problema asimmetrico difficile: dato N = p·q, è difficile fattorizzare N; p e q devono essere numeri primi grandi.
Operazioni di encyption e decyption sono semplici, e sono modular exponetiation. Questo può supportare sia l'encryption che la digital signature: posso modellare un crypto system ed avrò i due servizi a seconda dell'ordine delle operazioni.
Principio dietro RSA:
$m^x mod N$, c è un numero, quindi ogni messaggio viene tradotto in un numero, deve avere taglia $\leq$ N.
La funzione è periodica: se considero $3^x mod 10$ = {3,9,7,1,3,9,7,1,....}.Il periodo è lungo 4, se provo a cambiare m, la lunghezza periodo è uguale o minore: ese. $9^x mod 10$ = {9,1,9,1,..}, worst case period = 4.
Teorema di Eulero: computazione del max di $m^x mod N$, è la funzione Φ(N), più formalmente se m è co-primo con N (GCD(m,N) = 1), allora vale che $m^{\Phi(N)} mod N = 1$.
Computazione Φ(p):

- se p è primo, Φ(p) = p-1.
- se N = p·q, con p e q primi, avrò che Φ(p·q) = Φ(p)· Φ(q) = (p-1)·(q-1).
- Numero primo p^k, $\Phi(p^k)$ = (p-1)· p^{k-1}.

Conseguenza della periodicità: $m^x mpodp$ è periodica con periodo Φ(N)s. Prendo ad esempio $mod 11$, quindi $\Phi(11) = 10$.
Mi rendo conto che $9 \cdot 7 mod 11 = 2^6 \cdot 2^7 mod 11 = 2^{13} mod 11$. Quindi posso lavorare sull'esponente facendo mod Φ(N): $2^{13 mod 10} = 8 = 2^{3 mod 10} = 2^3$.
Conseguenza: $m^x = m mod N$ se x = $1 mod \Phi(N)$, in questo esempio x = 1 + kΦ(N).
Quando $3^x mod 10 = 3$? $3^5 mod 10 = 3$, ma l'equazione si risolve ogni volta che x = $1 mod \Phi(N)$.
Costruzione di RSA:

- Genero p e q primi grandi e li tengo segreti.
- Computo N = p·q e lo rendo pubblico, trovare la fattorizzazione è difficile (escludendo quantum computing la complessità cresce esponenzialmente con il numero di bit di N)
- Computo Φ(N) = (p-1)·(q-1), non posso computarlo conoscendo solo N, devo conoscerne la fattorizzazione. Ma ora ho il problema del mio recevier: la sicurezza di RSA risiede nel fatto che nessuno può computare Φ(N).

- Genero una public key e: 1 < e < Φ(N), e deve essere co-primo con Φ(N). (e è sempre dispari perché N è pari)
- Genero chiave privata d tale che e · d = $1 mod \Phi(N)$. Quindi $(m^e)^d mod N$ = m.
- Per risolvere: $m^x = m mod N$ devo risolvere x = $1 mod \Phi(N)$, ora ho $(m^e)^d$ = $m mod N$, devo risolvere $e \cdot d = 1 mod \Phi(N)$. Se conosco Φ(N) il problema è facile,altrimenti no.

Assunzione di sicurezza: dato N deve essere difficile trovare i fattori p e q, inoltre nno deve essere possibile computare Φ(N), e senza Φ(N) è difficile computare d ed e.
d è la chiave di decrypt (privata), mentre la chiave di encrypt (pubblica) è la coppia (N,e).
Perché funziona: se ti do N,e ed un messaggio cryptato $m^e mod N$, è difficile trovare x tale che $(m^e)^x mod N$ = m. Unico modo è fare brute force a meno che non conosci Φ(N). Problema dell'aritmetica $mod N$: le frazioni non si considerano, le soluzioni sono tutte intere.
esempio: p = 11, q = 17 (segreti), computo N = p·q, $111 cdot 17$ = 187. Φ(N) = 10·16 = 160 (segreto). Prendo e = 7, che è pubblico e primo con 160.
Ora, cerco d tale che e·d = 1mod160, in questo caso d = 23.
CHi computa ha la trapdoor (conosce Φ(N) che è quel qualcosa in più), rende pubblico N ed e. Per criptare M: C = $M^7 mod 187$, per fare decyption faccio $(M^7)^2 3 mod 187$.
Come funziona: sono la banca, genero p e q localmente e li moltiplico per avere N. Ora genero e e siccome ho computato io N, conosco Φ(N) e posso generare d. Dico all'utente di usare {N,e} come chiave pubblica, una volta fatta l'operazione mi tengo solo {N,e} d in privato. L'attacker può vedere il ciphertext, ma non può decriptare $m^e mod N$.
NB: messaggio numerico deve essere più corto di N (in termini di digits).
L'attaccante deve cercare tutti i numeri possibili: se riprova con e, ottiene qualcosa di diverso (non è symmetric encr, a meno che non conosca la fattorizzazione p e q), mentre per la banca è semplice perché ha la chiave privata d per decypt. N è grande, p e q anche. e può essere piccolo, mentre d è sempre grande: è utile spesso selezionarli entrambe grandi ma è possibile selezionare e piccolo (es = 3, così l'encryption è veloce). La probabilità che d sia piccolo è infinitesima, di solito si fissa una chiave pubblica e, da cui poi tanto si computerà d, non posso selezionare entrambe.
(Non raccomandato scegliere la chiave e piccola perché posso esserci attacchi, per ottimizzazione si può scegliere piccola, ma si apre a delle vulnerabilità).
Perché RSA funziona, trapdoor funciton: diventa facile computare $(m^e)^d mod N$ = m, con algoritmo di Euclide esteso:
assumo di avere due numeri coprimi, esempio 51 ed 11; GCD[51,11] = 1. Devo trovare a e b ∈ Z tali che 51·a + 11·b = 1.
1x51 + 0x11 = 51
0x51 + 1x11 = 11

Divido 51 per 11, segnando il resto: 4, r = 7. Prendo l'ultima riga, la moltiplico per 4 e la sottraggo a quella sopra:
1x51 - 4x11 = 7.
Ora divido 11 per 7, ottengo 1 con r = 4.
-1x51 + 5x11 = 4.
2x51 - 9x11 = 3.
-3x51 +14x11 = 1.
Ho trovato (a,b) = (-3, 14); complessità logaritmica, efficiente dal punto di vista computazionale.
Applico per computare l'inverso modulare:
ho e = 13 e Φ = 60, devo computare l'inverso di e: so che è co-primo con Φ(N), devo cercare $\Phi \cdot a + e \cdot b = 1$. Applico l'algoritmo di Euclide esteso e trovo (a,b)=(5, -23). La riscrivo isolando 13·(-23) = 1 - 60·5, ma l'uguaglianza vale anche per il modulo: $13 \cdot (-23) mod \Phi(N) = 1 mod(\Phi)(N)$, quindi ho trovato che d = -23 = 60 -23 = 37, quindi ora per decryptare mi basta elevare il ciphertext alla d.
RSA signature: prendo messaggio, faccio hash ed applcia DEC(H(M)). Quindi neòl caso di RSA faccio $H(M)^d mod N$, e mando il messaggio, la chiave pubblica e il TAG. L'altro end prende TAG, lo eleva alla e quindi ottiene $(H(M)^d)^e mod N$ = H(M) e può controllarlo facendo hash del messaggio.

10.15 Digital certificates and public key infrastrucutures

Digital signature: so come generare chiave pubblica e privata. Creo H(M) sul messaggio che voglio inviare, lo faccio perché la condizione per fare aritmetica $mod N$ il messaggio deve avere taglia più piccola di N, così lo ottengo. Trasformo il dato (encyption è termine improprio qui) facendo $H(M)^d mod N$: solo io posso fare questa computazione, ma chiunque può fare la trasformazione inversa $(H(M)^d)^e$ che mi fornirà H(M), ora computo di nuovo H(M) e controllo se torna con quello ricavato.

10.15.1 Problemi

Un attacker cerca di rompere la costruzione: prende q' e p', scelti da lui, computo N', genero chiave pubblica e' e chiave privata d', posso farlo perché conosco $\Phi(N')$. Modifico il messaggio M, faccio hash del così ottenuto M' e lo firmo con la mia chiave segreta d'. È vero che l'utente iniziale ha la chiave privata, ma l'utente finale deve avere la chiave pubblica e: L'utente finale ha già la chiave e salvata, ma come posso avere salvato ad esempio la chiave pubblica per un utente che non conosco? Devo per forza ottenerla dalla rete. Attacker può intercettare la comunicazione, dire di essere l'utente originale e rimpiazzare la chiave pubblica con la sua, e'. Quindi verificando il messaggio, questo è autentico ed è un problema.
Altro problema, RSA key transport: voglio connettermi alla banca con TLS, mando Client Hello e la banca deve mandarmi la chiave pubblica, scelgo una quantità random k e la trasferisco usando la chiave pubblica della banca.

Ma quando la banca mi manda la chiave pubblica, l'utente può mettersi nel mezzo e sostituirsi alla banca. Può farlo perché la comunicazione è attualmente in chiaro , quindi quando l'utente sceglie la random k, la manda criptata con la chiave dell'attacker, quindi attacker lo decrypta, lo legge e lo riencrypta con la chiave pubblica della banca rimandandolo a quest'ultima.
Ora l'attacker sa che il data exchange sarà criptato con la chiave k.
Problema anche in Diffie-Hellman: i due utenti Alice e Bob scelgono due chiavi e si mandano $g^x modp$ e $g^y modp$. Attacker si mette nel mezzo: sceglie una chiave z random, ferma la trasmissione di $g^x modp$ e genera $g^z modp$. Dall'altra parte, manda anche all'altro end $g^x modp$, quindi lo manda sia a Bob che a Alice.
Alice computerà una chiave $K_1 = g^{xz} modp$, Bob computerà $K_2 = g^{yz} modp$.
Ma l'attacker li ha entrambi: ha intercettato i due messaggi $g^x modp$ e $g^y modp$ quindi può elevarli alla z, che ha generato lui; attacker agisce da proxy.
Quindi ogni applicazione dell'asymmetric cryptography ha il problema del certificato della chiave pubblica: o ho TUTTE le chiavi salvate, oppure se devo recuperare la chiave dalla rete sono vulnerabile ad un MITM.
3 scenari differenti, stesso problema: ho un nome a cui è associata una chiave pubblica, tutti gli attacchi rompono l'associazione e cambiano una delle due parti. Bisogna legare, in termini di cryptographic bind tra il nome e la chiave pubblica.

10.15.2 Digital certificate

Digital certificate: qualcosa che mi permette di legare (in senso molto stretto) una chiave pubblica ad un soggetto, soggetto può essere persona, compagnia, entità legale. Devo fari si che l'associazione sia crypto binded, non rompibile.
Non si può risolvere il problema a meno di aggiungere un trick extra: non ho la crittografia attivata: i messaggi sono in chiaro, devo ancora attivare la crittografia.
Mi riferisco ad una terza parte fidata (certification authority), a cui chiedo : il nome è associato alla chiave pubblica?
Ma se la risposta avviene on-line, c'è il problema del MITM di prima.
Prendo il nome, la chiave pubblica e chiedo di firmare digitalmente il messaggio che contiene sia il nome che la chiave pubblica: es Flavia | 123456 diviene un unico messaggio digitally signed dalla certification authority, l'assunzione immancabile è la fiducia nella certification authority.
Certificato:

- Fase 1: sono una banca e voglio generare chiave pubblica e privata, devo farlo offline, non voglio trasmettere online nulla.Genero in locale e salvo in locale la chiave pubblica.
  A questo punto, offline, chiedo alla certification authority di firmare il nome della banca e la chiave pubblica.
  La CA è sicura che sia la banca a richiedere la digital signature: devi presentarti lì di persona, mostrando documenti etc..., fase complessa con aspetti legali.

Infine, mi arriva il certificato CERT = (Bank_Name, BankPK)$_{CA_sign}$, l'integrità del messaggio è garantito dalla digital signature della CA.

- Fase 2: un customer si collega alla banca, e questa mi manda il certificato, che contiene il nome e la pubblic key. In TLS avrò client hello, server hello e poi il certificato che contiene nome e public key che sono cryptographically bounded. Ora il customer deve assicurarsi che il CA sia trusted, nel PC c'è lista trustata: controlla nella lista e se è trustata deve controllare la correttezza della signature. Come faccio per fidarmi della digital signature: Browser - settings - security - manage certificates, si apre un box che contiene la lista di certificati fidati. Quindi cosa vuol dire fidarsi di una CA: la CA firma il messaggio che contiene (nome,PK) della banca, quindi c'è un messaggio e questo messaggio ha un HASH, e se uso RSA questo hash sarà elevata alla private key della CA, la chiave non è dell'entità d i cui si fa il crypto binding ma quella della CA. Quindi per invertire il TAG mi serve la chiave pubblica della CA, ma deve essere pre-installata nel PC, altrimenti sono soggetto ad un MITM. Quindi fidarsi della CA è molto forte: anche la public key della CA è nella forma di un certificato, quindi avrò crypto binding tra il nome della CA e la chiave pubblica. Ma chi firma questo crypto binding? Può essere self-signed, in quanto ci sono root authorities che non possono fare altro se non firmarsi il certificato da sole. In principio non bisognerebbe fidarsi della self-signed certificate a meno che non è firmato da una root authority.
  Trick per sito che vuole un certificato può essere self-signed, ma questo non vuol dire che sia vero.
  spazio utile: ssllabs per testare certificati dei siti.

Ma sono sicuro che sto parlando con la banca? Fin'ora ho solo verificato che la chiave pubblica inclusa nel certificato è associata al nome incluso nel certificato, ma chi mi di dice che il certificato me lo ha mandato la banca? Non è questo il ruolo del certificato: non mi garantisce che sto parlando con quel nome. Un attacco di questo tipo ha senso? Può avere ripercussioni il problema che chi sta dietro il certificato non è l a banca reale?
Quando l'utente manda la chiave pubblica, prima si è riferito al CA che ha fatto il crypto biding della coppia (nome | public key). Ora l'utente può prendere il messaggio e fare replay, ma non può sostituire il nome o la chiave e firmarlo, dovrebbe avere la chiave dell'utente. Quindi il certificato è sicuro: il messaggio è stato prodotto usando la chiave segreta associata al segreto, ovviamente l'attacker non può mandarti un certificato valido perché deve fare verifica offline burocratica.
Attacker non può più sostituire nulla nel crypto binding: l'associazione è forte, quindi risolve problemi della digital signature.
Risolve l'altro problema? Devo provare che l'entità con cui sto parlando possiede la chiave privata associata alla chiave pubblica. Come fare a dimostrare che possiedo la chiave privata associata al certificato? Chiedo all banca di firmare

qualcosa di fresco oppure chiedo alla banca di decryptare qualcosa di fresco. Quindi:

- Banca mi manda certificato con chiave e chiave pubblica, di cui verifico la certezza (è firmato dal CA). Posso ottenere ora la chiave pubblica della banca, e sono sicuro che sia autentica.
- Mando una nonce alla banca e chiedo di firmarlo
- Banca ritorna la nonce firmata con la sua signature.
- Ora applico la chiave pubblica ricavata prima per invertire la nonce che è stata modificata dalla banca per vedere se mi torna.

Ma ora faccio la duale:

- Banca mi manda il certificato
- Io trasformo la nonce usando la chiave pubblica della banca, chiedendo il risultato
- Ora, la banca mi manda il risultato pulito usando la sua chiave privata

Quindi, i certificati non garantiscono che la persona sia reale, ma un protocollo deve includere l'uso di certificati per poter provare l'autenticità dell'entità, in TLS uso i due meccanismi appena visti uno server side ed uno client side.
Approccio di TLS con RSA key transport:

- Ricevo il certificato dalla banca
- Non genero la nonce, bensì la chiave simmetrica che userò dopo in encryption. Mando la chiave criptata con la chiave pubblica.
- Ora posso scambiare dati criptati usando AES-128$_K$: quindi se eri la banca bene, puoi decyptare, altrimenti non puoi.

Difficile però includere diverse root authorities in un singolo PC, idea è di avere fiducia in una catena di certificati: mi voglio connettere alla banca, mi manda certificato firmato da un CA non in lista, quindi posso avere una gerarchia di CA, così vedo il certificato del CA che ha firmato quello della banca e vedo se è trusted.

10.16 Public key certificate

Public key certificate è una struttura dati che fa binding tra una chiave pubblica ed il suo legittimo proprietario. Approccio base: mi affido alle CA, che rilasciano CERT$_I D$ = binding del nome e della public key. esempio: sito web protetto con TLS: voglio proteggere l'URL del sito. Mi fido del certificato che mi viene fornito perché è rilasciato da un CA di cui mi fido. esempio: certificato di Bob: contiene chiave pubblica, CA identity CA$_i d$, CA signature del certificato di Bob.

Devo anche verificare che il server che mi manda questo certificato abbia la private key: mando challenge (nonce) e questa nonce viene firmata con la chiave privata del server.
Ora il protocollo di sicurezza può partire, questo ad esempio avviene in TLS.

10.16.1 Public key infrastructure

Un PKI consiste è il set di tools che serve per creare, distribuire, revocare un certificato per chiavi pubbliche.
Formato tipico per un certificato è X.509, ma per definire un PKI servono molti altri meccanismi: Public key Cryptographic standards, ogni PCKS#n è riferito ad un determinato servizio.
Formato del certificato X.509, definisce tutti i campi ed encoding per un certificato per chiave pubblica:

- version, altri dati: specifica la versione del protocollo (3 è l'ultima) e definisce altre cose:
  - validity period: il certificato è valido per un certo periodo di tempo
  - Serial number del certificato: ogni certificato deve essere unico, identificato con un serial number unico per la CA (è locale quindi per la singola CA)
  - Altre estensioni: posso inserire nel certificato altri parametri, esempio l'uso della chiave nel certificato.
- CA identity: chi è il CA che ha rilasciato il certificato. Rappresentato in modo gerarchico
  - Issuer: è in forma gerarchica, CN è l'ultimo livello, in questo caso è il full name della CA.
  - Subject: CN è URL del sito web che sto certificando (se ad esempio certifico un web server)
- User identity
- User public key: public key, formato dipende dall'algoritmo per cui sto certificando la chiave pubblica. Ad esempio se è RSA avrò i parametri pubblici di RSA, quindi l'esponente ed il modulo N. In DH: avrò quei parametri pubblici.
- CA digital signature: CA prende l'intero certificato e fa hash del certificato e lo firma con la sua private key: è quella legata alla public key della CA. La cosa importante è verificare l'autenticità del certificato: devo esponenziare questo campo con la chiave pubblica della CA e verificare.

Mi collego alla banca: mando HTTP GET in chiaro, ma invece di passare il messaggio direttamente a TCP lo passo a TLS (che è user library in user space) per criptarlo. Quindi parte TLS handshake.
Esponente RSA fissato: è provato che se seguo pattern binario la sicurezza è la stessa ma le prestazioni sono migliori (5 esponenti fissati).

10.16.2 Certificate Signing Request

Una certificate signign request è un messaggio mandato da un applicante ad una CA per avere certificato sulla digital identity.
Posso avere come approccio la generazione di tutte le chiavi fatta dalla CA, quindi anche la mia coppia private,public (cosa che succede nelle VPN), ma non funziona.
Il formato più comune per CSR è PKCS#10. Come funziona:

- L'applicant genera chiave pubblica e privata
- Genero CRS che contiene informazioni che identificano l'applicant, l'X.509 subject feild, le estensioni e la prova che posseggo la chiave privata. Quindi firmo con la mia chiave privata
- CA deve verificare che posso chiedere un certificato per il dominio che richiedo, non è una cosa standard:
  - Manda e-mail all'e-mail trovata come maintainer del domain, c'è un link di verifica
  - CA mi richiede di creare qualcosa sul dominio che mantengo, esempio creare un record .txt per quel dominio

  CA verifica la signature che ho fatto usando la mia chiave privata. Se tutto va bene crea certificato X.509, potrebbe inserire estensioni (a partire dalla versione 3): authority key identifier, subject key identifier, key usage (posso usare la chiave pubblica solo per una specifica azione), alternative names, basic costraint extension (molto importante).

10.16.3 Root certificates

Come certifico le CA? Anche la CA ha un suo certificato, e chi fornisce il certificato è un'altra CA. Struttura gerarchica, la root CA è il livello più alto della certification chain: è una CA che si auto-certifica l'identità. Un root certificate è un certificato in cui subject ed issuer sono lo stesso. Come posso fidarmi di un self signed certificate? Chiunque potrebbe farlo, quindi come faccio a capirlo: root certificates sono built in nel sistema operativo e non possono essere rimossi da utenti senza privilegi.

10.16.4 Certificate chains

In molti scenari reali, il certificato non è rilasciato dalle root CA, che sono poche quindi approccio non scalabile.
Uno o più CA intermedie: ho una catena di certificati, nella catena non ho per forza le stesse entità intermedie. Certificate chain è una lista di certificati che è formata da uno o più CA con una serie di proprietà (solitamente inizia con una end-entity certificate):

- L'issuer di ogni certificato matcha il subject del certificato successivo della lista
- Ogni certificato deve poter essere firmato con la chiave privata del certificato a lui successivo nella catena. esempio: la firma su un certificato deve poter essere verificata usando la chiave pubblica contenuta nel certificato precedente nella catena (dall'alto al basso della catena)
- L'ultimo certificato nella lista (quindi quello più alto) è la trsuted anchor, ovvero un'entità di cui si ha fiducia, esempio: una root CA.

Il chainign semplifica la verifica dei certificati, si usa una struttura ad albero in cui si raggruppano le CA's in modo che la verifica della radice e quindi del root CA verifichi anche gli altri livelli della catena.
A volte web server non mandano root certificate (perché può non essere nel SO).
Ma il chaining è pericolo? Ho una catena di certificati validi, posso generarne uno fake: creo un certificato fake ma legittimo e lo firmo con il CA finale (che sarebbe ad esempio il mio server).
Non è possibile: c'è un check, il basic constraint extension. Se nel campo certificate authority c'è NO (false) (e questo c'è nel certificato dell'end user) vuol dire che con la coppia chiave pubblica|privata non posso firmare altri certificati.
Wildcard certificate: Certificato valido per tutti i sotto dominii di tutto un dominio, esempio *.google.com perché in pratica una compagnia ha diversi servizi associati ai vari sub domains.
Periodicamente, le CA devono rilasciare una lista di revoca dei certificati, che gli utenti possono controllare. Come faccio ad ottenerla: inserisco la lista in una estensione specifica, distribution point da cui è possibile scaricarla.

10.16.5 Let's build our own authority

OpenSSL x.509: OpenSSL è toolkit crittografico composto da 3 componenti (librerie scritte in C). openssl ha variante di RSA basato sul teorema cinese del resto.
Alcune applicazioni vogliono un unico Ca certificate bundle con tutti i certificati: quindi metto tutti i file in uno solo, concatenando il root e l'intermediate.
Ora voglio provare ad usare Apache2 per configurare l'uso del certificato: proteggo il server http con i certificati che ho creato.
Apache2 supporta il meccanismo del virtual host: se voglio installare più web server su un unica macchina, avrei bisogno di più ip. Oggi posso avere più siti web su un unico web server con i virtual host.
ServerName è un field importante, serve per abilitare il virtual host.
Mi collego via browser e ricevo un warning: il certificato è valido, il browser/SO non ha la chiave pubblica della CA. Devo specificare esplicitamente https, nei siti noti c'è redirect automatico, voglio averlo anche io: lo metto nel file configurazione di apache2.

10.16.6 HTTPS Downgrade Attack

Siti ibridi, homepage in HTTP e login in HTTPS e questo era una vulnerabilità, homage non protetta è vulnerabile ad un impersonification attack: mi metto nel mezzo tra server e vittima, performo HTTPS con il server ma HTTP con la vittima.
Posso pensare ad un downgrade attack: identifico la vittima:

- Mi metto in mezzo alla vittima ed il default gateway.
- Faccio redirect dei pacchetti che hanno l'IP del sito localmente.
- La vittima si collega a me e replico con una versione del website.
- Faccio fare l'autenticazione

HSTS: Http Strict Transport Security: se provo a collegarmi ad un server con http, il server mi risponde di usare HTTPS, risponde con un cookie che specifica che devo usare https ed ha un tempo di fine (1h). Prima query è in chiaro, quindi da un punto di vista teorico la vulnerabilità rimane.
Alcuni browser web hanno incluso una lista di siti che contiene i siti più noti che supportano HSTS.
Non tutti i client supportano HSTS e c'è comunque vulnerabilità a DNS Spoofing Attack.

10.17 Diffie Helmann protection

Anche qui avevo il problema del MITM: Alice e Bob hanno g, p, e fanno exponentiation della loro chiave privata random x ed y.
Attacco è possibile: attacker selezione z e manda ad entrambi $g^z modp$ e quindi entrambi mandano la loro chiave all'attacker, quindi il data exchange passa per l'attacker nel mezzo (può ricavarsi tutte e due le chiavi per cifrare i messaggi e mandarli ai due end).
Senza dare nulla, l'approccio DH può essere attaccato via MITM ed è detto Anonymous DH.
IETF, protocollo BTNS (versione light di IPsec, Bettern Than Nothing Security), che è il DH Anonymous: so che c'è una vulnerabilità ma è meglio che non sapere nulla. Approccio base di DH è questo, quindi vorrei fixare il protocollo:

- Alice e Bob scelgono x ed y e chiedono alla CA di certificare i valori. Ovvero ottengo crypto binding tra il nome ed il valore di chiave pubblica. Ma x non è una chiave pubblica, bensì una quantità pubblica che corrisponde ad una quantità privata che solo loro hanno.
- Chiedo alla CA di ricevere qualcosa che è [Alice, $g^x modp]_C A$ e Bob, $g^y modp]_C A$.
- Ora attacker può generare z, ma non può sostituirsi ad Alice o Bob, perché non può ottenere il certificato.

Questo è il fixed DH exchange. Ho un altro problema: i valori $g^x modp$ e $g^y modp$ ora sono fissati, suppongo che mi collego alla banca nel 2018. Quando mi collego, avviene scambio dei certificati, il segreto che computo è $g^{xy} modp$. Mi collego nel 2020, ma non posso cambiare quantità x, perché il certificato è valido per una durata di anni (è processo legale che richiede vari step, non puoi farlo in 5 min): ogni volta che mi collego, computo sempre lo stesso segreto, quindi la chiave è sempre la stessa. Questo può o non può essere un problema, ma non è una best practice: ci sono nazioni che fanno attacchi severi, si salvano il tuo traffico per anni. Log del traffico dei cittadini: è criptato, ma aspetto per un tempo ragionevole e portò rompere la chiave privata dal tuo pc e scoprire il tuo traffico criptato.
Protocollo che non permette questo soddisfa la proprietà perfect forward secrecy.
vorrei non usare quantità fisse: se non faccio nulla, sono vulnerabile (DH anonymous), se certifico, ho fermato il MITM ma uso sempre lo stesso segreto nell'agreement (g^{xy}). Sfrutto il certificate chaining: Alice prende la sua public key, che ora è una standard public key usata in una digital signature e la fa certificare alla CA. Ma ora, ho la corrispondente chiave privata associata, quindi ora può produrre il termine $g^x modp$ e certificarlo con la secret key ed è diverso da un self-signed certificate: sto firmando altro, non una chiave pubblica. Associo il DH public coefficient con la mia identità e firmo l'associazione. Bob può prendere il valore, verificare che è firmato da Alice e può farlo recuperando la pub key di Alice, che è valida perché è firmata dalla CA. Quindi Bob verifica la DS di Alice, ma poi richiede il certificato sulla public key di Alice certificata dalla CA. Due quantità: il certificato CERT = [Alice, PubK]$_{CA}$, firmato dalla CA ed [Alice, $g^x modp$]$_{SK}$, firmato da Alice con la sua secret key. Ora evito il MITM: l'hacker non può fare nessuno di questi step. Questo è l'ephemeral DH. Quindi:

- Alice si fa certificare una pub key, a cui ha associato la private key
- Genera x, firma $g^x modp$ e lo firma con la sua private key.
- Manda a Bob il certificato standard della pub key più la firma che ha fatto lei sul coefficiente pubblico di DH
- È quindi possibile generare una x nuova per ogni connessione

Non c'è un singolo DH, ma 3 versioni:

- DH, MITM problem
- Fixed, long term secret
- Ephemeral, la migliore

In TLS:
DH senza nulla è la versione fixed, ma devo specificare l'algoritmo usato per la digital signature dalla CA: può essere RSA, DSS etc...

10.17.1 Symmetric vs Asymmetric

Nell'handshake, quando viene mandato il certificato:

- In DH non c'è certificato, solo 1 messaggio
- In fixed DH mando dopo il server hello il certificato e poi verifica di client
- In RSA key transport: mando il certificato e niente altro.
- Solo in ephemeral DH uso tutti e due i messaggi: mando certificato della Pk ed nel server key exchange mando g^x firmato da me.

10.17.2 Interlude: entity authentication con asymmetric crypto

Problema è che il certificato non basta, non è authentication perché chiunque può mostrarlo. La cosa giusta da fare nell'authentication è la prova che conosco la chiave privata legata alla chiave pubblica. Certificato è solo binding tra nome e chiave pubblica, ma l'authentication è veicolata dal fatto che conosco la chiave privata associata.
So come provare il certificato:

- Faccio digital signature di una nonce + ogni altro plaintext, e restituisco la signature fatto con chiave privata ed il certificato. Posso firmare solo se possiedo la chiave privata collegata alla chiave pubblica, ovviamente la chiave pubblica deve essere legata all'identità
- Uso encyption: mando public key all'authenticator, authenticator mi manda nonce + text ed encrypta usando la pub key e provo che sono autentico mandando indietro la nonce + ogni altro testo, dual approach. Ma se faccio MITM: vedo lo scambio dei 3 messaggi, ma dopo messaggio finale MITM può rompere la connessione e cominciare a parlare con l'authentication. Se dopo authentication proseguo con clear text, attacker può rompere la sessione e mettersi al posto del client. Ma se compito è aprire una sessione dopo l'authentication, devo fare altro oltre l'encryption per esempio AKA, ovver authentication and key agreement.
- Provo che so decyptare, ma oltre questo l'authenticator mi manda anche una symmetric encryption della challenge, includendo k nella asymmetric encryption. Ora, se posso scoprire k (e posso perché ho la chiave privata associata alla pubblica con cui è stata criptata la chiave) allora posso dimostrare di essere autentico risolvendo la challenge. Questo è ciò che viene fatto da TLS.

10.18 Ancora sul TLS handshake

Fase 3 dell'handshake (però non dirlo a nessuno perché è notazione del prof), il client risponde e posso autenticarlo, usando questo approccio:

- Server mi manda nonce, client risponde mostrando certificato e signature della nonce. Dov'è la nonce? Prima di questa fase ho avuto client hello e server hello, nel server hello è stata trasferita la nonce e questi messaggi sono utili per garantire che per sessione la nonce sia fresca

- Client key exchange: trasmette chiave simmetrica o le informazioni per generare la chiave server side (DH o RSA)

- Certificate verify, che deve contenere la firma della nonce + testo. Il fatto di cui mi interessa è che ci sia la nonce, se c'è altro non è un problema (applico hash per firma e poi manipolo quello). Devo includere signature della nonce, ma se aggiungo del testo, se questo testo è noto da server e client non da problemi. Idea interessante di TLS: includo anche la nonce del client, questo previene attacchi di tipo reflection migliorando la sicurezza. In muthual authentication devo fare crypto binding delle due direzioni della comunicazione. Posso includere anche il certificato, il server key exchange, il certificate request. Siccome uso TCP e so che i messaggi sono consegnati in maniera affidabile, posso creare un singolo grande messaggio che collega tutti i messaggi mandati e ricevuti nell'ordine. Metto client hello, poi server hello, poi certificate etc..., giustapposizione dei messaggi. Questo conterrà nonce del client e nonce del server. Siccome trasmissione è reliable ed in ordine il server avrà lo stesso ordine di messaggi, quindi avrà lo stesso grande messaggio. Firmo il messaggio e nel certificate verify mando il tag del messaggio grande.
  Se qualcuno prova a fare MITM e modifica client hello per fare ad esempio un downgrade attack o per rimuovere un cipher: ora il log a sender side diviene diverso da quello ricevuto dal server. Quindi anche se va tutto bene, quando firmo il messaggio, il server proverà a verificarlo e vedrà un hash diverso. Quindi includendo tutto il log (messaggi scambiati fin'ora) posso proteggermi da MITM o downgrade attack. Avevo risolto il downgrade attack sulla versione di TLS (usando 2 byte per ripete la versione di agreement), ma ora posso rendermi conto del cambiamento di ogni singolo byte per via della proprietà di anti-collisione dell'hash. Posso proteggermi da tutti i downgrade attack (anche detti biddown se attacco qualcosa di specifico, come rimuovere un chiper). C'è un però: è opzionale, certificate e certificate verify sono opzionali.

È quindi possibile risolvere questo attacchi biddown e downgrade una volta e per tutte: mando tutto in clear text, nel momento in cui passo a protected mode (encryption on) ripeto tutto lo scambio. Fase 4: sicurezza di TLS risiede nel messaggio finale: metto l'hash di tutto quello che ho visto fin'ora (fino al change chiper spec), quindi il server mi rimanderà finished; entrmabi proveranno di aver ricevuto tutto. Finish message è ciò che mantiene TLS sicuro. Serve per passare all'attivazione dell'encryption, ma la parte più importante è il messaggio di finish, in modo da evitare che qualcuno abbia fatto MITM.Authentication del server avviene in questa fase: prima d'ora non sapevo che il server fosse autentico.

Client authentication avviene nella fase del Crtificate verify, il server mi ha mandato la sua pubkey nel 3° messaggio, ma capisco che è autentico nella fase finale, quando mi manda il finish criptato con la chiave simmetrica k negoziata. L'autenticazione del server è in qualche modo implicita, capisco che sto parlando con il server reale solo alla fine.
Perché non è possibile fare encryption senza authentication (mentre il contrario sì)? Si romperebbe la sicurezza: c'è client e server. Sono attacker, mi metto come MITM. Prendo client hello, server hello, e gli altri messaggi... log interno. Prendo il log, cambio facendo downgrade o tolgo un chiper (ai messaggi del client), e mostro al server il log' risultante.
Ora client manda finish message, che è l'hash del log che è tsato criptato e integrity protected con i cipher scelti. Suppongo di avere TLS_X_WITH_RC4_NULL. Quindi alla fine della negoziazione, client non sa che c'è stato errore, quindi manda un enrcyption con RC4, quindi è paddato con keystream. Non c'è integrity: siccome MITM sa cosa ha trasferito al server, sa cosa c'è in log', Mette finish del client in xor con H(log) e xor con H(log') = $[\text{H(log)'}]_R C4$. Fa lo stesso anche con l'altro lato, quindi verso il client ed è game over.
Se disabilito integrità: grande problema, è necessaria per autenticare l'intera sessione. Pensarci bene perché è così che si protegge negotiation process / defeate negotiation attack. Secure negotiation: trasmetto dati in plaitext e li ripeto (tipicamente usando hash) quando l'integrità viene attivata.
Finish fa ancora parte dell'handshake, anche se è già criptato. Change chiper sec rimosso da TLS v1.3: protocollo più semplice mai fatto: 1 messaggio di un byte con un valore fisso costante (01), che serve per attivare cihper spec.

10.19 TLS key computation

Suppongo di aver adottato RSA key transport, la chiave simmetrica generata ai due estremi è stata generata dal client e trasferita via RSA. Chiave è generata dal client, ma chi sa se client ha i meccanismi corretti per generarla pseudorandom. Quindi problema della qualità della random key. In DH: chiave è $g^{xy} mod p$, ma sono sicuro che g^{xy} è uniformemente distribuita in 1,...,p-1. Non tutti i possibili esponenti possono essere implementati, non posso avere ad esempio g^{13} (devo avere prodotto di due primi). Problema di uniform distribution. Anche altro problema: servono più chiavi, una per encryption ed una per integrity, ma se mi serve IV serve altro random value: servono più chiavi e fin'ora ho solo scambiato un segreto.

10.19.1 Secret hierarcy

Gerarchia di protocolli seri:

- Pre master secret è quella generata da RSA o DH durante l'exchange se può essere sempre la stessa coppia client-server. Generato durante il public key exchange, è il segreto raw iniziale.

- Mischio la chiave alla nonce di client e server, ottengo il master secret. Così, anche se ho usato DH fixed so che il master secret cambia. Il pre-master secret può non essere perfettamente uniforme, ma master secret deve sembrare come un random value (voglio alta qualità). Risolvo il primo problema. È un segreto uniforme, pseudorandom.
- Ora mi servono più chiavi da una singola: in TLS ne uso fino a 6:
  - encryption
  - authentication
  - IV se necessario: ho due direzioni, da client a server e da server a client. Le chiavi di scrittura (se client invia a server) sono diverse da qielle di lettura (se client legge da server)

  Devo espandere il segreto, derivandone più chiavi. Posso fare abbreviated handshake in TLS, posso fare re-keying exchange: genero pre-master secret,che sarà valido per l'intera sessione, quando voglio aprire nuova TCP connection faccio nuovi client e server hello, nuove nonces client e server side. Prendo premaster, li estraggo ed espando generando le nuove chiavi che mi servono. Quindi cambio l'encyption key in ogni connessione TCP, tramite abbreviated handshake (c'è di nuovo finish message che è la parte più importante, evita ade sempio di rinegoziare due nonces uguali).

Extract then expand:

- Extract vuol dire aggiungere randomness nella generazione della chiave, aggiungo a premaster le nonces e genero la master key. L'idea è che la chiave deve essere uniformemente distribuita: es. AES uniformemente distribuita nel range 0-$2^{128} - 1$. Uso tecnica hash-like per abere output pseudo-random: equi probabile per tutte le possibili chiavi a 128 bit.
- Expand: una specie di PRNG che riceve un seed e lo espande come una sequenza illimitata di materiale pseudorandom. Se l'output è teoricamente illimitato posso tagliare a blocchi di ad esempio 128 bit ed ottenere le mie chiavi.

Quali funzioni usare: il blocco di expand deve essere una funzione buona, quindi sicura e veloce. Si pensa di poter combinare hash così da ottenere putput illimitato: mai combinare building blocks e fare qualcosa che non è pensato per quella specifica applicazione. TLS 2 errori:

- PRGN embedded nel codice e fissata, usava MD5 e SHA-1, male male. PRF è un algoritmo, va disaccoppiato dal protocollo, deve poter essere negoziato; questo può avvenire da TLS v1.2
- Hash functions poi rotte

TLS 1.2 usa PRF fa una 1-way hash, composizione buona ma non dimostrabile sicura: funzione di espansione (approccio naive). Derivo da un seme A_0, derivo gli altri A_i da un HMAC chaining ($A_i = A_{i-1}$). Si fa questo perché sembra essere più sicuro, quando Hugo Krawczyk (uno degli inventori di HMAC) vide questa applicazione, problemi: chaining accorcia la grandezza dei loop. Chaining non è una costruzione sicura.
Nuovo tool: Hmac Key Derivation Function (HKDF), pensato specificatamente per derivare le chiavi. Prendo HMAC ed uso un counter, non faccio più chaining;dimostrato che è sicuro, incluso in TLS v1.3. È possibile negoziare l'hash function usata nel PRF: TLS_DHE_DSA_WITH_AES-GCM_SHA256:

- Diffie Hellman in ephemeral mode
- Firmo Diffie Hellman con Digital Signature
- Il with entra nel dominio simmetrico
- AES-GCM cihper: authenticated encryption, quindi a che serve SHA256 finale se ho già integrity?
- SHA256: hash da usare nel PRF. PRF è algoritmo quindi non deve essere hardcoded, inoltre deve essere possibile negoziarlo.

HMAC usato in TLS v1.2 per uno scopo diverso da quello originale (non per forza detto che è usato male), quindi questa non è una buona pratica. Fino al 2010 non c'era una funzione di derivazione di chiavi (KDF) sicura, nuova costruzione HKDF, dimostrato che è sicura: funzione derivata specificatamente per key derivation. Sembra counter mode:

- Prendo master key, che è unica e ne devo derivare varie chiavi.
- Prendo hash function e costruisco la funzione di HMAC
- Messaggio:
  - prima parte è context string, arbitraria (es il mio nome). Se faccio solo $HMAC_K$(mio nome) è pseudorandom, non predicibile ma l'output è limitato a 256 bit se ad esempio uso SHA256
  - Aggiungo counter (esattamente come in counter mode), che permette di avere valori differenti

Metto context string perché, se ho la master key, ma se il SO ha negoziato la master key ed ora ho processi A e B che vogliono riusare la master key per negoziare le loro crypto keys. Ad esempio, se voglio rendere sicuro il mio sistema: uso TLS, metto nel SO il premaster/master secret negoziato e lo uso come sorgente per le chiavi dei miei processi. Ma se faccio HKDF = $HMAC_{MS}(0)$, $HMAC_{MS}(1)$,.. ma così se due processi generano le chiavi, avranno lo stesso set. Mettendo invece anche una label identificativa il problema non si pone. $HMAC_{MS}$(#process|0)...

In TLS v1.2: quando computo master secret input è premaster secret, label, nonces (client e server random). Quindi è $\text{HMAC}_{premaster}$(label | Nc | Ns | counter).
Quindi HKDF-Ciro = HMAC_k(Ciro | 0), quindi metto un identificatore del processo.
Funzioni di extrac ed expand? Si riusa HKDF per entrambe le funzioni in pratica, in teoria c'è analisi più specifica sulla fase di extract: questo perché la teoria della HKDF si rompe se si usa premaster nell'HMAC. Ci sono quindi meccanismi migliori per fare fase di extract, uso della stessa funzione è buona.

10.20 TLS connection management e supporto alle applicazioni

10.20.1 Alert protocol

TLS definisce messaggi speciali per fare alert (signaling) tra i vari field del pacchetto, possono essere in plain o criptati. BAD_RECORD_MAC è ad esempio errore fatal, mandato dal server quando integrity check fallisce. Ci sono vari alert, possono essere waring o fatal. Se è fatal la connessione termina, altrimenti se è warning il client può decidere di andare avanti o può proseguire.
Un alert è particolarmente importante: ricordo che TLS non protegge TCP, se invio pacchetto e c'è TCP header e TLS, la parte protetta con integrity e encryption è la parte TLS, la parte TCP è plaintext ed anche non protetta (non c'è integrità). Quindi attacker può cambiarla arbitrariamente. È possibile forgiare TCP reset packer e killare la connessione, spoofing dei segmenti TCP. Apre la porta al DoS attack. È più preoccupante un altro attacco, truncation attack: TLS fornisce encryption ed integrity, ma c'è il problema della session integrity. Non ho ancora discusso della sicurezza dell'intera sessione: client manda dati al server, attacker vuole far ricevere solo la prima parte di messaggio, quindi manda TCP fin, spoofing di un FIN, quindi chiude una connessione. Attacker fa trasmettere la prima parte e poi si finge il client e chiude con FIN spoofing. Server è sotto un attacco più sottile di DoS, session integrity, truncation attack. QUando analizzo protocollo, devo garantire non solo che encryption e integrity sono on, ma anche che l'intera sessione è protetta: all or nothing. In questo caso l'attacker fa si che il server riceva solo una parte del messaggio ed ha tolto l'ultima parte.
Come risolvere: quando comincio a trasmettere mando taglia, ma funziona solo se è preshared (in streaming non è possibile sapere la taglia a priori)
Aggiungo alert, signaling message, che fa il lavoro del FIN ma dentro sessione TLS, quindi con sicurezza attiva. Idea: mando dati applicazioni, quando ho deciso di terminare la trasmissione mando un messaggio di close notify, solo dopo questo mando TCP FIN. Siccome è alert message metto warining level, è una semantica half close, server manderà la sua close notify quando avrà finito.
Ora è possibile scoprire l'attacco: server sta ricevendo dati e poi arriva FIN, ma non ho visto close notify sono sotto attacco. Mentre se vedo tutti i pacchetti per bene e poi vedo close notify è ok.

Intergrity protection ha peso maggiore dell'encryption nelle applicazioni: non è tutto solo encryption.
Risolvo il problema della session integrity, ma non del DoS, ma almeno capisco che sono sotto attacco.

10.20.2 Renegotiation

Abbandonato in TLS v1.3, in TLS originale idea era: mando TCP connection usando una chiave, poi un'altra con altra chiave... definivo una singola TLS session con singolo handshake + handshake abbreviati dopo il primo.
Non è l'unica cosa da fare, perché funziona bene solo per connessioni TCP piccole.
Oggi le TCP connection solo lunghe e vorrei cambiare la chiave ad un certo punto. Posso farlo solo se inizio una nuova connessione TCP, come faccio a farla entro una già esistente. Vorrei anche cambiare livello di sicurezza della sessione: parto da AES-128 e poi voglio passare a AES-256.
Renegotiation imlementata in TLS:

- Parto con handshake iniziale
- Sono in encryption exchange, ma mentre scambio i dati parto con un renegotiation handshake all'interno della stessa sessione.
  Il messaggio di renegotiation ora è protetto, sono in TLS session
- Dopo renegotiation avrò una nuova sessione TLS con nuovi chipers e nuove chiavi

In teoria, il renegotiation handshake non è distinguibile da quello iniziale. C'è problema tecnico: se sto scrivendo del testo e mi arriva un renegotiation: come viene gestito il testo dai buffer TLS e TCP. Posso exploitarlo? Analyst Mash Ray: white box analysis, code review di TLS. Trova bug che può permettere attacco, ma il problema non è della versione di TLS bensì de protocollo. Bug era molto "creativo", quindi nessuno si prese la briga di fixarlo. Dopo averlo letto, studente scoprì come sfruttarlo.
Regola d'oro: rendere i protocolli semplici.
Bug: attacker apre TLS session col server e manda dei dati. I dati sono generati dall'attacker in plaintext e sono criptati in TLS session. Quando client comincia a parlare col server, in realtà attacker ha fatto MITM: attacker manda la negotiation all'interno della sua TLS session. Server pensa che sia una renegotiation: switcha ai nuovi parametri usati.
Quindi il client manda i dati, attacker ha messo preambolo a questi dati ed il server crede che il messaggio sia legittimo.
Dopo la creazione della sessione, attacker non può fare nulla, ma ha creato situazione di plaintext injection attack. Può fare injection di dati prima di quelli generati dal client.
ATtacker fa MITM col client, quando client apre TLS connection l'attacker salva messaggio in buffer, apre TLS connection col server, fa plaintext injection al server e poi forwarda il messaggio al client.

In teoria non si può fare molto con plaintext injection, se applicazione è semplice: vittima manda messaggio in cui vuole comprare la pizza, autentica con un cookie il messaggio. Attacker non può modificare il messaggio, ma può aggiungere preambolo: attacca HTTP, aggiungendo X-ignore-this dopo la newline, così da ignorare l'ordine nella get e lasciare solo il cookie di autenticazione.
Attacco all'API di twitter: twittava in chiaro password degli utenti.
Per prevenire renegotiation: immediatamente disabilitato, poi patchato, nel 2010 standardizzato. Renegotiation extension: cercare di far si che server possa riconoscere una renegotiation è crypto binded alla precedente, include finish della sessione prima; era di nuovo un esempio di session integrity.

10.21 Altri dettagli sulla sicurezza dell'RSA key transport

RSA key transport è un po' un bordello, quindi si è abbandonato il metodo.
RSA key transport:

- Server mi manda RSA pub key
- Client cripta il premaster secret con la pub key (premaster calcolato prima). È un encryption scheme, che non garantisce integrità e la tecnica non è robusta a chosen chipertext attack

Chose chipertext attack: tutte le operazioni sono fatte *modn*. Attacker vede C $= M^e$ e si chiede se può criptare C, servirebbe M $= C^d$, ma non ha d. Assumo che attacker può accedere ad un decryption oracle, che può decriptare tutto tranne che C. Come posso decriptare se ho un oracolo così fatto, scegliendo un chipertext? Posso dare qualunque C' diverso da C: scelgo valore random r, faccio $r^e modn$, faccio poi $r^e \cdot Cmodn$ = X. Mando X all'oracolo, X è diverso da C e mi ridà X^d, mq ora ho $(r^e \cdot C)^d$ = r·C^d. Ho scelto io r, mi basta dividere per r, ma sono in aritmetica modulare, siccome è difficile che r sia coprimo con n quindi posso fare inverso modulare: $r{-}1modn$: faccio $X^d \cdot r^{-1}$ = M.
Proprietà di non malleabilità: un chiper è non malleabile se preso un encrytion C si qualche messaggio M, l'attacker non può creare un chipertext differente C' che si decripta in un messaggio M' che è legato in maniera sensata ad M.
Fix di RSA: padding, standard PKCS #1, primo standard per la famiglia PKCS, ovvero public key criptography Standard, specifica RSA encryption e decryption.
Primo probelma: suppongo m = 1, C= $m^e = 1^e = 1$. Chipertext è uguale a plaintext.
Secondo problema: ho un oracolo che può fornirmi il cihpertext. Cosa accade se dopo 10 giorni vedo un chipertext che è uguale ad uno precedente. RSA soddisfa IND-CPA? No, vengono introdotti dei tricks, costruzione del vero RSA (non della versione Vanilla):

- Aggiunta di due byte all'inizio: 00 02. Metto poi 8 byte random e diversi da 0 (suppongo sia IV), in modo che due messaggi identici hanno ciphertext differente, protezione da CPA. Delimitatore di quantità random, che

è 00. Dopo lo 0, partono i dati. Risolvo il problema di criptare ad esempio il messaggio 1 e risolvo il problema del CPA, ora la capacità di RSA è ridotta rispetto al $modn$ (ho meno valori possibili, visto il padding)

- Quindi ora, quando client risponde al messaggio del server, usando la pub key per criptare, cripterà il premaster secret con il padding.
  In SLL v3 specification: viene detto che quando server prova a decriptare il messaggio e se la decodifica non torna (formato non è corretto), invia abort message. Se decription funziona, vai avanti.

Sembra un Padding Oracle: mando un messaggio che specifica problema nella sicurezza, perché c'è un abort o un go on. Non è un'informazione grandissima, ma tanto basta.

10.21.1 Bleichenbacher's Oracle

Adaptive Chosen plaintext Attack, 1998. Ha scoperto che se è possibile ripetere più volte un chosen ciphertext attack basato sui messaggi visti prima, è possibile decriptare qualsiasi messaggio se ne ho 2^{20}. Target up in SSL v3.0, corretto in TLS v1.0+, ma non sei protetto da side channel attack, difficile correggere del tutto il problemi. In giro almeno fino al 2019, rimosso in TLS v1.3
È un CPA, obiettivo è decriptare un chipertext C: C = $M^e modn$, in RSA è pericoloso decriptare C perché M è il premaster secret.

- Scegli r e costruisci un nuovo chipertext
- C' = C$r^e modn$ = $(Mr)^e modn$, RSA vanilla. Modifica meaningfull del messaggio M, operando sul ciphertext applico l'operazione al plaintext.
- Sto chiedendo all'oracolo, che è il server, se il messaggio inizia con 00 02: se decryption fallisce, la modifica non è corretta, altrimenti vuol dire che è corretta ed ottengo informazioni.
- Server è l'oracolo: manderà abort oppure procede with the session.

È possibile usare l'informazione del messaggio con questo leak.
Toy example: padding di RSA è il seguente: l'inizio del messaggio è 0 o 1, ho solo 8 bit come stringa iniziale. Oracolo mi diare se $(M \cdot r)$ comincia con 0 o 1. Rivela il primo bit, bastano $log_2 n$ query per decriptare l'intero messaggio. esempio: p = 13, q = 19, n = 247 (8 bit). Prendo e = 29, d = $e^{-1} mod 216$ = 149. Assumo di vedere C = 90, cos'è M: $90^{149} mod 247$, ma attacker non ha d. Può fare la seguente cosa: testo se un messaggio di mia scelta inizia con 0 o 1. Mando al server 90 $\cdot 2^{29}$ = C', questo è $(C \cdot 2)^{29}$, 2 è il mio r. So che questo C' è $(M\ cdot 2)^e$, faccio test per vedere se 2M inizia con 0 o 1. Attacco in questo caso non è nemmeno adaptive, posso fare 2M, 4M, 8M... sto testando sempre se il plaintext $2^i \cdot M$ inizia per 0 o 1. Server mi dirà: {0,1,1,1,0,1,1,1}, quindi $2M modn$ inizia per 0 e così via... Ora, assumendo che il modulo fosse 256, avendo messaggio M = 11010001, quindi se fosse lineare, starei scoprendo

bit per bit, ma non è questo il caso.
Quando mando al server $(2^i \cdot M) modn$, lo decripta e mi dice qual'è il primo bit, come attacker non so nulla, il messaggio che voglio scoprire è fra 0 e 246. Provo tutti i valori tra 0 e 246: moltiplico per 2 e faccio modn, mi rendo conto che da 64 in poi inizia per 1, poi a 123 ricomincia da 0. So che 2M inizia per 0 solo se M è in un certo range. Provo con (2M,4M), ottengo i range per le coppie (0,1), (1,1), (1,0), (0,0). Mi interessano le coppie (0,1), ad ogni step scarto dei valori. Alla fine riesco a scoprire tutti i bit e scopro il valore.
RSA è sicuro quanto un singolo bit: se posso rivelare un singolo bit di un messaggio, RSA è rotto.
Corollario: è possibile attaccare la parità, ovvero se numero M è pari o dispari.
In Bleichenbacher's oracle servono molti più messaggi, in quanto la matematica dietro è più complessa, devo testare se messaggio inizia per una stringa molto più lunga.
Attacco sempre pratico: client trasmette i dati, attacker si salva la sessione, e sa che valore ha mandato (il premaster secret criptato). Dopo 10 giorni attacker comincia: manda il primo messaggio C' per sapere se inizia con 00 02. Posso riprovare dopo un tot di giorni. Messaggio non cambia, è sempre quello: attacco non è nella sessione di TSL, ma alla creazione della sessione, il client ha finito di trasmettere. Attacco funziona perché coppia chiavi (pubblica,privata) non cambia nel tempo.
Attacco fu scoperto nel 1998 e corretto in TLS v1.0+, ma dopo questo vennero scoperti una miriade di side channels: alla fine lo stesso Shamir consigliò di deprecare RSA in TLS.
2016: DROWN attack. Alcuni siti permettevano ancora downgrade a SSL v2, salta fuori che è peggio: due casi

- Server supporta SSL v2 downgrade, combinarono oracle a studio dei server, 17% dei server permettevano SSL v2
- Public key e private key erano le stesse del server: è come migrare il server, in quanto miglioro la sicurezza usando versioni migliori di TLS e lasciare in un altro server la stessa chiave, e questo secondo server può essere dowgradato. Riuso del certificato, ovvero attacco il server debole per rompere quello più sicuro. 16% dei server erano vulnerabili

ROBOT attack, 2018. Hanno Bock (consultant), comincia a testare Facebook servers. Conosce bene crittografia. Facebook supporta TLS v1.2, 1M loc, se ricevo RSA PKCS, TLS risponde in maniera propria. In 1M di loc ci sono eccezioni, molta attenzione al main software path, ma se mando un messaggio fatto male: ora il sw deve rispondere, il codice entra in side exception handling, che solitamente è meno testata. Bock scopre che mandando un messaggio valido o non valido e creando errori nel messaggio poteva ri-creare situazione in cui padding oracle Bleic. ritornasse. Protocol fuzzying: provare con parti random di un web server se è possibile triggerare vulnerabilità.
Facebook fixa vulnerabilità, ma Hanno ne trova un'altra, quindi si affida ad amici che fanno systematic analysis e scoprono molti altri server vulnerabili.

Implementazione di TLS è una jungla (cazzo!)
Contromisure:

- Cambiare completamente il padding, quindi ripensare completamente il deploy di RSA
- Careful implementation

Soluzione: dimenticare TLS.
Take home: implementation è tricky, gli errori possono durare a lungo. Errore era in SSL originale, c'era Oracle ma senza saperlo.
Secondo messaggio: storia molto simile al MAC-then-encrypt, anche qui ho CCA, difficile fixare questo tipo di errori, si finisce per rimuovere il protocollo. Practical security (cross site scripting, SQL injection, buffer overflow), ma non si capisce sempre crypto attacks.
Dopo ROBOT's penetration, chi scoprì l'attacco andò dai siti web a dire di stare attenti ma quelli risposero che usavano military grade encryption. MALE MALE MALE.

10.22 The failure of certificates

Problema del mondo reale: certificati fake. Certificati sono controllati da entità esterne diverse da quella per cui è rilasciato il certificato. I CA sono trusted: posso verifiare che il certificato è valido, ovvero che la signature della CA è valida e poi ricorsivamente controllo che la firma del sito web è valida.
Oggi l'assunzione che la CA è trusted è un assunzione non certa: gli attacker sono anche i governi, c'è evidenza che ci sono attacchi e monitoring a larga scala fatti dal governo.
Se governo forza una CA ad emettere un certificato fake: emette certificato che corrisponde a google.com, di cui la private key è posseduta dal governo così che possa controllarlo. Ora l'utente ottiene un certificato fake: fa i check della CA e della private key del server e questi funzionano. Scenario divenuto reale negli ultimi 10 anni: può essere emesso ad esempio per la sicurezza nazionale, se ottengo certificato per un sito noto (esempio google.com) posso monitorare tutti i cittadini.
Ci sono evidenze di certificati fake emessi per google, quindi il punto è che se ho degli attacker più potenti e può controllare CAs, non tutta la catena ma solo una parte locale, allora il PK model è debole. Come aggiungere extra-check: problema fu scoperto da Google, aggiunta di un DB gigante che chiamo certificate transparency DB, che contiene tutti i certificati del mondo. Se ho questo DB, chiunque può accedervi e fare un check, quindi attacco può essere violato.

- Governo crea un certificato fake e non lo inserisce nel DB. Quando certificato arriva all'utente, questo checka le firme ma anche se il certificato è nel DB. Non lo trova e riconosce che è fake.

- Attacker ottiene certificato fake e lo include nel DB. Ma Google checka DB periodicamente, sa quanti certificati sono rilasciati a suo nome e si rende conot che ce n'è uno fake. Richiede la revoca.

Security è data da due attività di monitoring: lo user controlla se il certificato è nel DB, ma lo fa anche la vittima dell'attacco (per esempio Google).

10.22.1 Merkle Trees

Approccio usato anche in blockchain.
Come rendo sicuro un file:

- Prendo crypto hash function, e creo footprint del file.
- Rendo sicura la fingerprint: o lo copio offline in una penna usb (dispositivo di storage in generale), altrimenti metto digital signature l'hash. Posso lasciare la digital signtaure online, nessuno potrà ripetere l'operazione visto che ho incluso la mia private key.

Se file è grande, alla fine del file metto una signature. In p2p systems, divido il file in chunks e trasmetto un pezzo alla volta, solitamente out of order. Come posso essere sicuro che il chunk è valido: la signature è valida per tutto il file e devo scaricare quella, ma per verificare l'integrità devo anche avere tutti i chunk, Quindi posso farlo solo alla fine del download. Approccio non scalabile, inoltre qui devo solo verificare l'interno file, ma spesso devo solo verificare una parte del file.
Perché non usare una signature per ogni chunk, funziona ma:

- C'è un overhead computazionale molto più grande.
- Storage overhead, se il chunk è relativamente piccolo c'è un overhead bello largo. es RSA2048 = 256 byte in più. In Bitcoin si usa signature basata su elliptic curves, ECDSA256 = 2x256 bit = 64 byte che non è comunque trascurabile
- Non c'è più integrity check per l'interno file: se verifico tutto il file sono sicuro, ma se verifico i singoli chunk non sono sicuro. Strip type attack: mando 6 chunk, attacker toglie 3 di questi e non possono sapere se ho ricevuto tutto il file o no. Session integrity problem: l'intero messaggio deve rimanere non modificato. Servono delle strutture apposite per verificare che sia stato ricevuto tutto, esempio seq_num/tot chuncks.

Ho un file: se ne faccio hash ed ottengo fingerprint, e poi firmo il fingerprint, una strada per poter assicurare tutto il file è fare hash di tutto il file. La sicurezza è compromessa se faccio hash delle due metà e poi faccio l'hash delle due metà? Intuitivamente non cambia, ma non è così. Approccio di Merkle: Hash tree, divido il file in 8 parti e faccio hash dei singoli pezzi: H(A), H(B), H(C)...
Ora prendo hash di A e B e li riassumo in un hash univoco: H[H(A), H(B)], posso ora fare il merge con H[H(C), H(D)]: H[H[H(A), H(B)], H[H(C), H(D)]]

conterranno cripto summary fino a D. A questo punto faccio il merge finale con l'altra metà e firmo l'hash finale: posso verificare i singoli pezzi se conosco qualcosa extra: voglio verificare solo C, ma non posso farlo con solo C: se ottengo H(D), H[H(A), H(B)] e H{H[H(E),H(F)], H[H(G), H(F)]}, i siblings di C. Mi serve root ed i 3 siblings per poter verificare C (numero di siblings logaritmico): trust anchor è il root. Devo sempre fare fingerprint del file, e il modo di farlo è usare Merkle tree: ma in goni caso il primo step è avere root del Merkle tree. Ora posso o mettere il root in uno storage sicuro oppure metterlo pubblico dopo digital signature.
Se devo verificare il file per intero devo scaricare tutti i pezzi ed avere il fingerprint ma questo dovevo farlo anche prima. Ho aggiunto complessità, ma è limitata e posso verificare ogni singolo chunk, mi servono solo i siblings.
Applicazioni: fornisco un certificate, ho un DB di certificati. Ottengo root certificate ed 3 siblings: root è uguale per tutti, ma associo al certificato i siblings che mi permettono di verificare il certificato.
Suppongo che mi diano un chunk C e creo un pacchetto che contiene C, S1 S2 ed S3 ed ho il root fuori dal pacchetto. Può un attacker modificare C così che abbia lo stesso hash dell'originale o modificare i siblings così che diano lo stesso hash? Anche i siblings possono non essere sicuri: se modifico i dati, non posso modificare C in C' così da avere lo stesso hash (anticollision), devo modificare direttamente l'hash. Posso modificare tutti i sibling in modo da avere l'hash che torna sempre, ma finché il root è salvato in una USB o digitally signed, se non posso modificare questo non posso avere modifiche che riescono a corrompere il file finale.
Approccio molto efficiente per molte applicazioni:

- Blockchains, usato ma bisogna fare altro. (Dominio del Dunning-Kruger).
- Google's Certificate Transparency.
- Molte altre.

Altro esempio: ho un milione di dispositivi e voglio mettere un codice, e che nessuno lo modifichi. Integro il codice, S1, S2,... S20 ($1M = 2^20 = 20x256$ bit = 5120 bit extra). Ho root signature, la espongo su sito pubblico e posso verificare che il device non è modificato usando Merkle tree: prendo codice e lo mischio con S1, poi con S2 etc...
Sistema distribuito per node authentication incredibilmente scalabile.

10.22.2 Merkle's tree extension con il tempo

Uso time slots: raccolgo tutto il materiale che voglio certificare all'interno di questa time window. Alla fine della giornata, faccio girare Merkle's tree e rendo sicuro il root. Giorno dopo: raccolgo i restanti certificati e li metto insieme i un root. Ora posso unire i root e rendere sicuro solo il merge dei due root. Quindi in questo modo creo dei blocchi di certificati, ogni giorno vado avanti così.
Idea della blockchain: Metto in ogni blocco un Merkle Tree root: cripto summary della transazione, le transazioni sono organizzate con Merkle Tree. Il

blocco successivo fa Merkle Tree del blocco precedente.
Posso verificare le transazioni senza scaricare il contenuto dei blocchi, sicurezza risiede nel fatto che l'hash del blocco finale è sicuro: è il trust anchor e finché è sicuro nessuno può falsare delle transazioni.

10.22.3 Certificate transparency

Ho il DB gigante di Google con tutti i certificati, rendo possibile che chiunque veda la satessa lista di certificati.
Nel processo normale:

- Sito chiede al CA di verificare un certificato
- Durante l'handshake il client verifica il certificato

Ora, il sito chiede il certificato all CA: CA crea il certificato e lo sottomette al log server (huge DB con tutti i certificati), che mi ridà certificato con i siblings. example.com vuole il suo certificato: la CA crea il certificato ma poi va dal log server per farlo includere nel Merkle Tree e di ricevere i siblings per poterlo verificare. Questo richiede ovviamente del tempo (viene fatto offline).
Ora, CA ha il certificato di example.com più i siblings, parte supplementare necessaria. Ora example.com ha il certificato e le informazioni extra necessarie per verificare il certificato nel Merkle Tree senza scaricare gli altri certificati. I siblings sono in chiaro, ma non possono essere modificati in maniera meaningfull perché il root è protetto.
Quindi client verifica firme di CA e del server e poi usa i siblings per verificare (basandosi sul giorno, c'è timestamp che dice in che blocco mi trovo).
Iniziativa iniziata nel 2013: in quell'anno si è capito che i governi fanno casini.
Quindi: PKI non è sicuro contro attacchi scalabili e molto grandi ed una soluzione possibile è usare transparent database: combinazione scalabile di chains of block + Merkle's tree, ma non risolve il fatto che nel DB ci sono solo dati veri, serve altro e questo è risolto dalla vera blockchain.

10.23 TLS v1.3

Maro 2018: RFC per l'IETF in modo da standardizzare la versione v1.3. Oggi, pochi usano 1.3 ma perché ancora non c'è migrazione completa di TLS 1.2
Cambiamenti in TLS v1.3:

- Rimossi tutti i cipher vecchi: RC4, 3DES, SHA-1, MD5 ed anche AES-CBC. Rimosso tutto tranne AEAD: paradigma che permette di avere authentication and encryption in un singolo algoritmo. esempio: TLS_AES_128_GCM_SHA256: AES_128_GCM usato per AEAD e SHA256 per key derivation function. Niente più MAC then encrypt, per evitare chosen ciphertext attack
- Goal di TLS v1.3 era di avere un sistema che garantisse la perfect forward secrecy: suppongo di avere un server e qualcuno può avere accesso alla chiave privata.

Ogni volta che c'è asymmetric criptography, la private key deve essere sicura. Ma può accadere che la chiave viene scoperta prima o poi. Nel caso di perfect forward secrecy se nel caso in cui la chiave privata viene leakata, c'è garanzia che qualsiasi cosa hai fatto nel passato rimane nascosto, non può essere decryptato.
Con RSA questo non può accadere: ho server, che mi da la chiave pubblica. Client genera il premaster secrete lo trasmette al server. Avversario può fare logging del messaggio e lì c'è il premaster secret. Se qualcuno riesce ad ottenere la chiave privata, il messaggio che è stato preso precedentemente può essere decryptato ed rivela il permaster secret.
Ad ogni sessione cambia il premaster, ma uso sempre la stessa chiave pubblica per criptarlo.

Hearthbleed: vulnerabilità che permette di fare request per un oggetto che causa un buffer overflow, es un oggetto di 4byte ed io ne chiedo 40000. Se il sistema non controlla i limiti, la memoria ritornata sono i 4 byte dell'oggetto più altre aree di memoria che non dovrei vedere. TLS, in particolare la versione di openSSL, era rotta: pagine di memoria di cui potevi vedere il contenuto. Come è possibile che un implementazione major per TLS e in cui gli sviluppatori sono forti, non si sono resi conto del check missing per buffer overflow. Commit che ha causato il problema: 31 dicembre 2011 alle 23:00, colpa dell'errore umano, ma scoperto 2-3 anni dopo.

10.23.1 Garantire PFS nel TLS handshake

Non posso più usare RSA, ma non posso nemmeno usare fixed DH (X ed Y sono fisse) e neanche anonymous DH.
Rimane solo ephemeral DH: il server ha certificato della chiave pubblica ed usa la public key per mandare $g^y modp$, che è firmata dal server. C'è chiave privata del server e la CA con la sua private_key$_{CA}$, due quantità segrete. Assumo che ad un tempo T, l'attacker riesce ad ottenere la chiave della CA. Può decriptare messaggi ad un tempo $T_0 < T$?
No, perché mi servirebbe anche l'altra chiave: posso fare un MITM visto che ho la chiave del server, ma non posso andare indietro nei messaggi.
Anche se ho private key del server, posso impersonare il server: non posso ottenere una chiave g^{y_0}, perché dovrei invertire il Dlog.
Quindi se uso DHE posso avere PFS, questa è l'unica tecnica che posso usare di tutte quelle viste: ho quindi sempre 3-way handshake contro 4-way handshake, non devo negoziare l'asymmetric encryption. Il client nel client hello chiedeva al server se usare come asymmetric crypto algorithm RSA o DH:

- RSA: server deve mandare pub key etc...
- DH: server manda g^y e client g^x etc...

Ma ora il server non deve più scegliere quale algoritmo asimmetrico usare, si usa sempre DHE.

- Client: DHE coefficient g^x, Nonce$_c$, ciphersuites (e gruppi, oggi si usano solo curve ellittiche)
- server: DHE coefficient g^y, Nonce$_s$, selcet mode: ha tutto ciò che glie serve, può partire con l'encryption mode, in quanto ha anche scelto l'algoritmo da usare per encryption ed integrity.
- cert request, cert$_s$, signature con cert$_s$, finished(HMAC).
- Cert$_c$, signature con cert$_c$ finshed(HMAC)

Molto più semplice, c'è meno scelta ed il protocollo è molto più simmetrico.
Side effect interessante dell'encryption anticipata: i certificati, ovvero l'identità di server e client, non sono mai trasmessi in chiaro quindi ho identity protection.
Grande differenza tra TLS 1.2 ed 1.3 è che rimuovendo RSA e forzando l'uso di DH si ha un handshake abbreviato.

10.23.2 Pre-shared key

Perché usare una chiave pre-shared, se era stata rimossa da WEP: preferisco un premaster secret sempre diverso.
Nella community di TLS c'era una discussione infuocata sull'usare una chiave pre-shared in alcuni scenari, in cui non serve avere asymmetric encryption o è costoso (ad esempio in una sensor network). Aggiunta della possibilità, quindi opzionale, per supportare la pre-shared key: viene decisa offline e computata solo al primo handshake. Se mi collego alla banca, posso pensare di fare abbreviated handshake, ma solo sulla stessa sessione. Se mi ricollego dopo un certo tempo relativamente piccolo, potrei aver mantenuto la chiave in cache e potrei volerla riusare (NB: PMS è diverso dalla PSK).
C'era già in TLS 1.2, mentre in TLS 1.3 viene aggiunto un supporto opzionale: derivo PSK per la sessione 1, per la sessione 2 etc... L'attacker riesce ad ottenere la chiave per la sessione 3.
K = HKDF$_PSK$(N$_c$, N$_s$) se uso solo la PSK non ho PFS. Il problema di autenticazione è quello più serio, il client può non avere un certificato, quindi vuole usare DH anoymous quindi conviene almeno avere PSK. Ma qui l'idea è: il client offre al server una PSK identity, siamo in anonymous DH. Se associo un termine anonimo g^x con un segreto per-shared statico, il server può mandarmi g^y e può computare HKDF$_{PSK}$(N$_c$, N$_c$, $((g^x)^y)$), le session keys sono computare dinamicamente usando qualcosa legato ad un anonymous DH exchange.
Quindi: client e server non hanno certificati, possono ricavare una chiave k pre-shared? Client e server usano anonymous DH, ma invece di generare la chiave da g^{xy}, che è attaccabile, lo usano per accordarmi su un hidden session nonce, input in più per il HKDF. K$_{sess}$ = HKDF$_{PSK}$(N$_c$, N$_c$, $((g^x)^y)$).
Sessione 1: g^x, g^y, generiamo K$_{sess}$ = HKDF$_{PSK}$(N$_c$, N$_c$, $((g^x)^y)$). Qualcuno riesce a scoprire PSK, ma per computare k devo conoscere g^{xy}, ma questo non è loggato, è conosciuto solo dai due peers. L'autenticazione è garantita dal fatto

che abbiamo la pre-shared key, quindi la sfrutto per avere perfect forward secrecy con una chiave statica e senza certificati; non servono le firme o i certificati, mano messaggi necessari.

10.23.3 Handshake

- Client hello
- DH, PSK, extra data, application data se c'è PSK
- Server hello
- DH key share
- Ecnrypted certificate + certificate verify, finished
- Ecnrypted certificate + certificate verify,
- Dati

0-RTT data: sopratutto Google si è interessato nell'accelerare l'handshake. https:www.google.com: quanto serve per mettere su HTTPS session, server TCP handshake (SIN, SIN-ACK,ACK), poi client hello, server hello, CKE, finished. Quanto tempo passa, è tutto signaling: 1 RTT per TCP, +2 RTT per TLS, quindi posso trasmettere dati dopo 3 RTT. È possibile ridurre al minimo? Avere solo RTT della TCP connection: comincio a mandare dati applicativi subito dopo aver aperto la connessione, 0-RTT. Se non uso encryption, posso farlo tranquillamente: se uso http posso mandare messaggi non criptati, ma posso farlo criptando subito dopo? È possibile usando pre-shared key: mando SIN, SYN-ACK, ACK. Mando messaggi dopo ACK in cui dico di usare la pre-shared key, la mia nonce ed i dati (che possono essere applicativi). Posso applicare $\text{HKDF}_P SK(\text{N}_c, \ ...) =$ key e la uso per criptare i dati applicativi e la chiave è nuova ad ogni nuova sessione. Mischio per la nuova chiave la nonce, il coefficiente pubblico del client e i cipher offerti.
C'è vulnerabilità: riesco ad ottenere vantaggi dal punto di vista della velocità delle richieste HTTP, una volta ottenuta la risposta posso scaricare la pagina criptata, salvo molti RTT. Replay attack ovvio: c'è solo la nonce del client. Per essere sicuri, bisognerebbe generare il segreto usando entrambe le nonce. Se è possibile supportare questa vulnerabilità è ok, ma c'è comunque il rischio.
0-RTT, se uso su un sito già visitato, posso riusare una pre-shared key già computata: la prima volta devo calcolarla, ma poi posso salvarla in cache.
Mitigazione di 0-RTT: non posso risolverlo, unico modo è includere la nonce server side, potrei fare controllo sul nonce reuse, ma servirebbe un DB assurdo difficile da mantenere in un sistema a larga scala.

10.23.4 Altro su TLS 1.3

- Non c'è più re-negoziazione: attaccata, dopo il fix è stato rimosso. Introdotta tecnica per key upgrade.

- HKDF è ufficialmente incluso: inventato nel 2010 ma non mandatory
- Management di EC semplificato
- Rimozione della compressione.
- Exported key: quando setto un premaster secret e poi master secret e delle chiavi derivate vorrei poter usare in diverse applicazioni la PMS, API apposita per farlo.

11 IPsec

Parentesi su VPN: IPsec non vuol dire VPN, IPsec è solo un tool per costruire VPN.
VPN: Virtual Private Network, utili perché magari abbiamo diverse reti, separate geograficamente ma che vorremmo avere in un'unica rete virtuale: ho una rete in Francia ed una in UK, vorrei poter assegnare gli IP della stessa subnet ad entrambe. Posso creare una linea dedicata p2p, ma è costosa. Non sono nella stessa operating network, tra i due branch ho l'Internet: diverse rete amministrate come AS, non posso gestire le informazioni di routing. Inoltre Internet è non sicuro per design, obiettivo è di creare una VPN su Internet.
Virtual Network: device non sono nella stessa rete ma è come se lo fossero.
Tunneling: prendo un pacchetto e lo metto come payload di un altro pacchetto. Ad esempio metto IP in in altro pacchetto IP: il pacchetto interno è "nascosto": il routing è fatto sul pacchetto più esterno. Tunneling risolve il problema del routing, ma non il problema della sicurezza.
Quindi uso tunneling sicuro: se posso usare tunnel sicuri nella VPN, allora sono sicuro anche se non posso configurare i gateway intermedi. Esempio: TLS tunnel, è tutto autenticato e criptato, le due enrity che comunicano sono autenticate.
IPsec è una possibilità di costruire una VPN perché rende il tunneling sicuro.

11.1 IPsec components

È layer di sicurezza, offerto da diversi protocolli, che è inserito fra il layer di trasporto ed il layer di rete(IP): stra fra plain IP e layer 4.
Differenza tra TLS, che sta tra livello 4 e 5: le applicazioni devono essere consapevoli che c'è TLS sotto: se uso HTTP non posso usare porta 80, ma devo usare 443, quindi devo esserne consapevole; in IPsec non è così. IPsec protegge l'intero host, mentre TLS solo il playload HTTP.
Diverse implementazioni:

- Estendo layer IP per supportare IPsec, miglior approccio ma difficile da deployare
- Bump in the stack: aggiungo layer addizionale, approccio di Linux

- Bump in the wire: costoso, serve hardware addizionale, ma non devi modificare sistemi legacy. Inietto il pacchetto in un device che implementa IPsec

Seconda grande differenza con TLS: TSL è un protocollo all-in-one: RFC specifica tutto, architettura, negoziazione etc... IPsec è una suite di protocolli, ci sono diversi protocolli in IPsec, è un'architettura per sicurezza dei sistemi.

11.1.1 Security association

Associazione logica tra due host che vogliono proteggere il traffico, non è per forza tra due host ma può anche identificare come proteggere traffico tra due router: definisce come proteggere il traffico tra due device che hanno IPsec abilitato.
Associazione è mono-direzionale, se voglio protezione bi-direzionale servono due associazioni. È un set di parametri, internamente IPsec specifica dove salvare i parametri, c'è security association DB, in cui si salvano tutte le security association.
La main key della SA è il Security Parameters Index, ma si usa anche l'address a cui la SA è associata (receiver side).
Ci sono anche molti altri parametri, come faccio il retrieve della SA dal SAD: ho due approcci per inserire la SA nel DB

- Associazione statica
- Associazione dinamica

Quando ricevo IPsec packet protetto, devo cercare la SA nel DB: ho la chiave SPI, identifica la SA ma non è l'unico parametro usato per costruire la chiave. SI usano anche src e dest addresses, longest match-like approach.
Come derivo e scambio encryption ed integrity keys in IPsec? Come faccio a configurare le SA, in TLS c'è handshake: obiettivo è autenticare le entità e scambiare le chiavi. Ipsec supporta due modalità:

- Manuale: sys admin deve configurare SA e security policies del router. Devo installare la setssa SA anche nell'altro gateway con cui voglio creare la SA. Se non è gestito dallo stesso sys admin, c'è un modo per trasferire i parametri all'altro end-point. Non è solo problema di scalabilità, se lo faccio a mano devo anche refreshare le chiavi ogni tot (è più sicuro fare rekeying ogni tot per evitare alla lunga dictonary attacks). Va bene in uno scenario piccolo, ma se scenario è più complesso voglio qualcosa di automatico
- IKEv2, protocollo per configurazione automatica. Vantaggi rispetto alla configurazione statica: creazione on-demand SA, quando mi serve triggero la configurazione automatica per negoziare la chiave.

11.1.2 Protocolli di IPsec

Protocolli di sicurezza di IPsec

- AH per autenticazione, può esserci o non esserci nell'implementazione di IPsec
- ESP per encryption ed encapsulation, nella nuova versione dello standard è l'unico mandatory

AH ed ESP i principali: all'inizio ESP forniva solo encryption, ora fa entrambe e quindi non ha senso averli entrambi. Ma nel passato non era così.
Le due modes più supportate sono transport mode e tunnel mode.

- Trasport mode: se proteggo IP packet in trasnport mode, metto AH tra l'IP header originale ed il resto del pacchetto. Se uso ESP metto l'header tra header IP e header TCP/UDP, alla fine dell'application data metto ESP trl e ESP auth.
- Tunnel mode: creo il tunnel e proteggo cosa è nel tunnel: con AH proteggo il nuovo IP header, in ESP proteggo sempre il nuovo IP header.

Perché ci sono entrambe: tunnel mode ha più overhead, quindi perché usarla. Transport mode si può usare solo quando end points dell'IPsec SA sono gli stessi che generano i pacchetti, es proteggo traffico IP di un client ed un server, che implementano IPsec. Nel caso in cui sono generati da altre macchine, es routers, non è detto che implementino IPsec. Se voglio gateway to gateway protection devo usare tunnel mode.

11.1.3 IPsec protecion e access control

SA dice come proteggere il pacchetto, ma non quali pacchetti proteggere. Security policy: applicata ai pacchetti e specifica se il pacchetto deve essere protetto o no. SP sono set di regole salvate localmente in un security policy database. Ho quindi due DB: SPD e SAD. Security policy è una "match-action" rule che specifica cosa far con pacchetti non protetti
Action

- Pass, non fare nulla
- Scarta
- Usa IPsec procotol e mode

Match: combinazione arbitraria di

- Ip src
- Ip dest
- Protocol

- L4 src/dest
- Altre specifiche a seconda dell'implementazione

Output packets: pacchetto viene generato ed arriva al layer IPsec

- Checka se c'è policy che matcha nel SPD
- Se c'è una policy, fa quello che è specificato
- Packet è usato per cercare SA nel SAD, se metcha una policy
- Una volta trovata la SA, proteggo il pacchetto. Se uso IKE e non trovo SA viene triggerata la negoziazione

Input packet

- Cerco un match nel SAD
- Processo il pacchetto (encryption, integrity)
- Checko SPD per vedere se ci sono policies

11.2 IPsec security protocols

11.3 IPsec on Linux

Voglio creare una VPN gateway-to-gateway che protegga la comunicazione tra due siti VPN. In Linux, IPsec implementato nel kernel dalla v2.6.1.
C'è set di user space tools

11.4 IPsec security Protocols: AH/ESP

AH: Authentication Header

- Fornisce solo autenticazione, sia per payload che per header
- Meccanismo anti-replay

ESP

- Authentication come in AH
- Encryption
- Traffic flow confidentiality

11.4.1 AH

Struttura AH: quando uso AH ho 51 nel campo protocol dell'header IP. Nell'header AH

- Next Header: dipende dalla modalità di IPsec: se è tunnel mode ho l'header dell'altro pacchetto IP, altrimenti il protocollo di trasporto

AH autentica sempre tutto l'header, in tunnel mode abbiamo un header aggiuntivo (slides)
Integrity check: c'è il MAC del pacchetto, ma non è computato su tutti i field dell'header: c'è payload, ma non tutti i valori, perché alcuni mutano nel tempo, ad esempio il TTL, il ToS, fragmentation etc...
Quindi questi field sono impostati a 0 nell'header AH. Algoritmo usato per computare ICV: è negoziato o configurato a mano nella security association, qualunque scelgo di usare, deve essere multiplo di 32 bit.
Sequence number in IPCsec? I pacchetti IP possono essere consegnati non ordinati, ma questo è un problema per l'encryption, inoltre se non abbiamo una nonce: posso fare replay di IP packet. Siccome IP non distingue i duplicati, serve supporto esplicito nel AH header.
Seq num: 32 bit, standard dice che se attivo la feature devo fare rekeying del SA quando finisco i numeri di sequenza. Feature opzionale: extended seq num: 64 bit, c'è counter interno che è la parte alta, mentre nel pacchetto uso solo parte bassa.
Anti-replay: slinding window, se ricevo pacchetto che è prima del lower bound, viene scartato. Se invece è più alto dell'upper bound: accetto il pacchetto ma shifto a destra. Quando raggiungo il massimo: devo startare da 0, se configuro a mano devo riconfigurare SA. Meccanismo di anti-replay è opzionale.

11.4.2 ESP

Protocol = 50, ESP autentica solo payload, header e trailer, encryption solo sul payload e sul trailer. Header IP non è autenticato né criptato.
Padding: 2 ragioni

- Se usiamo block ciphers, serve che plaintext sia multiplo del blocco
- Il ciphertext risultante deve terminare su una boundary di 4 byte

Siccome padding è variabile, serve un campo che dice quanto è lungo.
Anche qui encryption ed authentication algorithm consigliati sono listati. Si può usare AEAD, quindi field del ICV non serve.
IP non garantisce ordine: se uso encryption che fa chaining fra i pacchetti, potrei perdere dei pacchetti, anche ad esempio l'IV va messo nel pacchetto, prima del data payload, e bisogna tenere traccia del fatto che l'ho messo.
ESP fornisce anche traffic flow confidentiality: con analisi statistica della distribuzione dei pacchetti per derivare dei fingerprint specifico per i vari data traffic. Non buono per la privacy, ci sono due contro-misure:

- Possibilità di alterare la taglia dei pacchetti, aggiungendo padding addizionale ai pacchetti
- Dummy packets: pacchetti fake, in questo modo cambio il fingerprint del mio traffico. Serve meccanismo per distinguerlo da quelli veri

11.5 IKEv2

Se uso IPsec, devo salvare lo stato nei nodi

- Quale servizio di sicurezza usare
- Quale crypto algo usare
- Quali crypto keys usare

Gestione manuale non scala, ma in ogni caso l'approccio è debole: SA a vita, cosa che non va bene.
IKE: protocollo per negoziare dinamicamente la SA. Stabilisce dinamicamente e mantiene la SA
Fasi di IKE

- Prima fase in chiaro, obiettivo è negoziare la SA che sarà usata per proteggere lo scambio successivo
- Autentico il pacchetto mandato prima (tipo il finished di TLS)
- Child SA: fase due di IKEv1

Quindi, due tipi di SA

- IKE SA: usate per scambiare in maniera protetta i messaggi IKE successivi
- CHILD SA: SA per scambiare i dati.

IKE usa UDP su porta 5000 o 4500, c'è meccanismo di retx apposito.
IKE header: major e minor version, quando mando il primo pacchetto: l'initiator specifica le due versioni del protocollo che implementa (minor e major). Quindi l'altro end invierà la sua scelta, come in TLS $\Rightarrow$ man in the middle downgrade.
C'è flag di IKE: version bit, messo a 0 se uso la versione massima possibile, setto ad 1 se non è quella più alta supportabile. Initiator dice che vuole usare Versione N, suppongo che responder supporti N-1. Quindi initiator si accorda per N-1, flag è messo ad 1.
Nel caso del MITM: i due peer si rendono conto che stanno usando versioni minori e fermano la comunicazione.
Meccanismo non supportato in IKE v1.
IKE init phase

- Richiesta in clear text seguita da risposta in chiaro. Vengono negoziati i parametri di sicurezza per l'IKE_SA, mandando le nonces ed i valori di DH.

- Output: generazione di una seed key, che verrà espansa per generare tutte le chiavi necessarie per la SA.

Ci sono più IKE payload concatenati fra loro: secutiy association payload, key exchange payload, nonce payload ed un opzionale payload per autenticazione (supporto ad x.509).
Key generation: ho la chiave generata nello scambio, che è generata con prf(N_i, N_r, g^{ir}), prf è negoziato.
Vengono generate 7 chiavi con prf esteso, come avviene in TLS.
IKE vulnerabile a DoS: genero molti init packet con IP spoofati, bisogna generare molte chiavi, bisogna anche salvare lo stato dell'initiator quindi è possibile drainare la RAM o saturare la CPU. Meccanismo di difesa di IKE basato su cookie 4-way handhsake: responder risponde con un cookie, senza salvare nulla. Quindi initiator manda riposta autenticata con dentro il cookie. Funziona perché l'IP address è fake, quindi pacchetto viene inviato ad un nodo diverso. Inoltre, il cookie deve essere stateless: il cookie può essere verificato senza salvare nulla. Cookie è un hash della nonce initiator, del SPI e dell'IP, più il segreto, che sta nel responder. Per verificare che il cookie che torna indietro è valido, il responder si ricomputa l'hash.
AUTH phase: si autenticano tutti i messaggi precedenti, si verifica anche la private key in caso di certificato di autenticità.
CHILD SA: posso generarne quante ne voglio

12 Secret sharing

Overview di modern crypto, che è oltre la confidenzialità e l'integrità. Non è più solo encrypt ed autenticate, ma ci sono nuovi servizi si security e privacy.
Il secret sharing è una tecnica per diffondere un segreto fra diverse persone.

12.1 Trivial secret sharing

Tecnica banale, non è stata inventata da qualcuno. Obiettivo: io ed un mio amico, voglio condividere un segreto con il mio amico, ad esempio dividendolo in due parti così che ognuno dei due ne abbia una parte.
Idea base: lo spezzo a metà e do una metà per uno. Non va bene: se il segreto è ad esempio di 8 bit, splittandolo in due se l'attacker può intercettare una delle due metà ha un vantaggio: se originariamente l'attacker poteva indovinare con prob = $\frac{1}{256}$, ora la probabilità diventa $\frac{1}{16}$. È possibile fare meglio: trivial secret sharing, prendo il segreto e genero una sequenza random e faccio l'XOR del segreto e della quantità random: X = R $\oplus$ S. Do ad uno dei due il random, all'altro do l'XOR del segreto. Se li rivelo entrambi, mettendoli in XOR posso ricostruire il valore originale del segreto. È anche immediato che una delle due parti, ovvero il random, non contiene informazioni su S. L'XOR da leak sulle informazioni di S? IN teoria si, ma se R è truly random pad, ed S è plaintext, l'XOR è one time pad, Vernam cipher one time pad, quindi è sicuro. X non rivela nulla su S se R è truly random.

Quindi, solo combinando le due informazioni posso avere il segreto, ma nessuno dei singoli amici ha informazioni sul segreto.
È possibile avere anche variazione: suppongo che segreto sia una quantità compresa fra 0 e 255, posso fare la stessa cosa che ho fatto con l'XOR con l'aritmetica standard, posso fare $(S-R) mod 256$. Quindi, dopo avere generato truly random value, computo la quantità ed a questo punto do la RAND ad uno dei due e all'altro do $(S-R)$. Modulo non è necessario, ma pratico: se uso standard CPU in cui registri sono a 32 bit, le operazioni interne sono $mod 2^{32}$, punto importante è che il numero non è per forza un primo (tipo posso usare 256).
Si può estendere ad n persone: il dealer ha dei segreti, che deve condividere dando 4 shares a 4 parties, in modo che se un attacker intercetta fino 3 shares, sono comunque sicuro al 100%, (probabilità di indovinare il segreto non cambia). Computo un segreto, 3 random e computo S - R_1 R_2 R_3. Se intercetto una delle R_i, ho 0 informazioni: se ad esempio ne intercetto 2, ottengo S - R_i, dove R_i è la rand che mi manca. Questo è il trivial secret sharing, per ricostruire faccio la somma $mod 256$ (sto ragionando su un segreto di 1 byte). Perfect secrecy fino a n-1 shares rivelati, perfect secrecy: la probabilità di indovinare prima di vedere uno share è uguale alla probabilità prima di indovinare lo share.

12.2 Shamir secret sharing

Se devo sharare un segreto fra n parties e basta, allora non si usa Shamir, è un overkill. Uso piuttosto trivial secret sharing. Problema: nel (n,n) secret sharing scheme ho un dealer, ho le n parties ed ogni partyha uno share, alla fine ricostruisco il segreto tramite le n share, uno da ogni party. Supponiamo di dover dare una password a tutti i parties: do uno share ad ognuno, ora voglio ricostruire la password o segreto solo sulle informazioni di sotto-insieme dei parties.
(t,n) sheme: la popolazione è n, ma bastano t di loro per poter ricostruire il segreto, con $t \leq n$ (se $t = 1$, ogni party ha la chiave).
Ci sono 11 scienziati, hanno un progetto segreto e vogliono lockare il segreto in una cassaforte, in modo che se ce ne sono 6 di loro possono aprirla. Quanti lock vanno messi sulla cassaforte, e quante chiavi servono. Servirebbero 462 lock, ed ogni scienziato avrebbe bisogno di 252 chiavi (sono i valori minimi).
Basic building block in diverse costruzioni crittografiche: è anche possibile avere group crypto, voglio ad esempio mandare messaggio ad un gruppo di persone. Shamir e Blakley, due soluzioni indipendenti, ma quella di Shamir è ottima rispetto a quella di Blakley.
Idea di Shamir: schema (2,n). Problema geometrico: se ho due punti, ho un equazione di una retta: se ho coorindate x ed y di un punto, infinite linee passano per questo punto. Ma se ho un secondo punto, una ed una sola linea li attraversa entrambi.
Definisco il segreto come f(0), dove f è l'equazione della retta. Secret è $y = f(x)$, con $x = 0$. Se ho 4 persone, l'unica regola è di non avere un punto sull'asse y, quindi ognuno ha come share un punto (x_i, y_i). Se intercetto un solo valore, non posso derivare l'equazione della retta, ma con due punti posso ottenerla, ed

ottenere S. Posso avere un numero arbitrario di persone, con t = 2.
Procedura di dealing:

- Il dealer conosce e decide il segreto, determina le shares e le distribuisce. Il dealer costruisce una retta y = S + a·x, con a truly random. Quindi, facendo f(0) = S.
- Se ad esempio voglio nascondere un segreto S=39, genera un a=15, e y = 39 + 15·x
- Quando un nuovo party arriva: il dealer può dargli un qualunque punto che abbia x > 0, ad esempio 1,2,3... e ne derivo lo share che sarà il punto (x,y).
  Ogni party conosce il suo share, ma può anche conoscere le coorinate x degli altri parties, non gli da informazioni in più riguardo il segreto.
- Per ricostruire: lo schema è (2,n), ovvero mi bastano due punti: $\frac{y-y_j}{y_i-y_j} = \frac{x-x_j}{x_i-x_j}$

Estensione a (t,n): posso generalizzare, è vero che una retta è identificata in maniera univoca da 2 punti, ma una parabola: 3 punti, un cubo: 4 punti etc...
Schema (t,n) è un polinomio di ordine (t-1), concettualmente le cose sono identiche.
La complessità sta nel trovare una formula di interpolazione valida per un polinomio generico: interpolazione di Lagrange, sistema che permette di ricostruire l'equazione di un polinomio di ordine arbitrario avendo un numero di punti arbitrario+1.
Ogni polinomio di grado t-1 con t punti noti può essere decomposto come $y = \sum_{i=1}^{t} y_i \Lambda_i(x)$, dove $\Lambda_i(x)$ è il polinomio di Lagrange, che è implementato come segue: $\Lambda_i(x) = \prod_{m=1, m\neq i}^{t} \frac{x-x_m}{x_i-x_m}$, il prodotto è effettuato scartando tra le x_i proprio la x_i.
$\Lambda_i(x)$ è una base orto-normale, quindi $Lambda_i(x_i) = 1$, mentre $\Lambda_i(x_m) = 0$ se m $\neq$ i.
$\Lambda_i(x)$ mi da la y_i solo sul mio punto x_i, ottengo quindi uno spazio vettoriale.
Schema (t,n)

- Dealer: se t è il mio obiettivo, seleziono un polinomio di grado (t-1) p(x) = s + a_1x + a_2x^2... , dove gli a_i sono interi.
- Devo avere almeno t shares, ad ognuno degli share do (x_i, y_i) tali che $y_i = p(x_i)$
- Per ricostruire: collezioni le t shares, che corrispondono a t differenti valori della x e computo l'interpolazione di Lagrange ad x = 0. $\Lambda_i(0) = \prod_{m=1, m\neq i}^{t} \frac{-x_m}{x_i-x_m}$.

Lo schema è sicuro? Non è esattamente Shamir secret sharing: non c'è segretezza. Vorrei che lo schema sia sicuro: devo provare che S può essere qualunque valore. Questo non è vero: mi metto nella condizione di aver perso uno share, ho visto solo due di questi. Per essere unconditionally secure, il segreto dovrebbe essere un valore uniformemente distribuito, faccio il seguente attacco: metto nel parametro mancante il valore d, quindi ottengo s = 476 - 3·d. Faccio trial and error sul valore di d ed ottengo alcuni valori di s. Finché conosco 2 dei 3 shares, posso dire qualcosa sul segreto s. Quindi lo schema non è unconditionally secure; non è questo il vero schema di Shamir. Se ho meno di t-1 shares, dovrei avere 0 informazioni riguardo il segreto: la probabilità che avevo prima di conoscere le shares non cambia.
Nell'esempio del file Mathematica: P(before) = $\frac{1}{100}$, la P(after) cambia: colleziono share 1 e 2, ottengo equazione s = 476-3D, quindi a seconda della D, avrò alcuni valori che vengono scartati: ottengo dei valori di S solo se la D è un numero reale, ma so che le shares sono interi. Restringo i valori ad un sottoinsieme di quelli possibili. Quindi lo schema non è unconditionally secure.

12.2.1 Vero schema di Shamir

Bisogna usare l'aritmetica modulare, usando come mod un numero primo. Allora lo schema è unconditionally secure. Conseguenza del vero schema di Shamir:

- Aritmetica modulare con un numero primo è fastidioso: le CPU fanno mod 2^{32} o 2^{64}, quindi non primi. Serve introdurre un'aritmetica modulare apposita, quindi ho modifico il processore o lo faccio in sw: è un problema. Quindi per questo motivo se bisogna fare uno schema (n,n) ricordarsi dello schema triviale

- Modular arithmetic prime p large: mi ricordo del dlog, quindi mi aspetto che anche qui sia grande. I problemi sono diversi: discrete log, RSA fanno riferimento a quello che si chiama computational security ovvero problemi difficili da risolvere, ma possono essere risolti se ho una potenza computazionale sufficiente. La complessità di RSA si adatta alla potenza di calcolo che cambia nel tempo, ma in questo caso, selezionando un valore p primo ottengo la perfect security, può anche essere piccolo. La sicurezza non è legata ad un problema computazionale, bensì alla probabilità di indovinare s con t-1 shares = probabilità di indovinare senza le shares.

esempio: se il segreto è scelto in un range(0, 100), scelgo 101 come p. Per calcolare i Λ_i devo applicare gli inversi modulari $mod 101$. Siccome ho usato un numero primo p, nel momento in cui provo i vari d ottengo gli stessi valori che ottenevo prima.
Quindi, schema di Shamir si basa interpolazione di polinomi, usando aritmetica modulare e mi da perfect security. È anche efficiente? Il criterio di efficienza è detto idealità: qual'è la taglia degli share che posso gestire?
Prendo un segreto S = 1001 1101, lo divido in due parti, ognuna mi da 4 bit di informazioni. L'attacker deve quindi scoprire solo i restanti 4 bit. Nell'XOR,

una parte era il valore random e l'altra parte era l'XOR. Può una share essere di taglia minore di un segreto, ad esempio di 6 bit? No: un segreto ha 8 bit di informazione (informazione legata all'entropia) se truly random, share 1 da 0 informazione da sola, ma quando aggiungo share2 devo aggiungere 8 bit di informazione, quindi deve portare da sola 8 bit di informazione e quindi essere lunga 8 bit. Quindi l'ultima share deve avere la stessa taglia del segreto, perché deve avere la stessa informazione. Ma può essere più grande: esempio, la proposta di Blakley le taglie degli shares sono t volte la taglia del segreto. Lo schema di Shamir è ideale, in cui la taglia degli shares è uguale a quella del segreto, quindi l'ottimo.

12.3 Secret sharing for secure multiparty computation (SMC o MPC)

Iniziata nel 1982, pionieri sono i ricercatori israeliani. Posso fare computazioni sui dati senza vedere l'input ma con la possibilità di computare l'output?
esempio: 3 persone stanno monitorando degli accessi ad un certo IP address. Ho un manager, che fornisce l'accounting e non è interessata agli accessi individuali, bensì al totale degli accessi. Tutti pensano che l'unico modo di fare la computazione è sommare gli accessi monitorati da i singoli utenti. Problema: la compagnia deve essere una third party trusted, se ho requisiti di privacy. Quindi c'è la convinzione che serve un third party trusted, ma non posso avere una cloud operation in cui opero su dei dati che sono protetti, ovvero non vedo i dati ma alla fine riesco a computare il risultato.
Idea: ho un certo numero di accessi, creo due sistemi indipendenti. Sono sicuro che l'autorità A è l'università, la B è il LUG e per esempio il valore è il rating dato ad un professore. Come faccio a sapere di essere sicuro hce ci sia la privacy? Problema risolto con uno scagnozzo al centro di calcolo che opera come trusted party, ma se qualcuno rompe il delphi, si ha accesso a tutti i dati dell'utente.
Il trusted third party deve essere trusted, inoltre anche il sistema deve essere trusted (in questo caso il delphi), fino all'anno scorso era vulnerabile.
Soluzione crittografica: creo i due server, uno del Delphi ed uno secondario Delphi2 o pippo, gestito da un'authority differente. So che le due authorities sono differenti e non si scambiano i dati fra di loro. Con queste ipotesi, devo solo essere sicuro che le due authorities non colludano. Posso usare il seguente trick: schema (2,2), scelgo un modulo appropriato, ho random ed s-random,ad esempio $mod1000$, il party one da all'authority A la random e all'altro s-random. Da soli hanno 0 informazione, unendoli ricostruisco l'informazione segreta. Quindi chi fa il monitoring è anche il dealer: genera il dato segreto s e da le shares ai parties, così che ogni authority abbia le shares da tutti i parties. Le authorities possono sommare i valori delle shares ed hanno 0 info, ma se li sommo ottengo la somma originale ($mod1000$). Posso fare una somma senza vedere i valori originali, facendo si che le due authorities avessero le shares. In pratica: uso la proprietà lineare che la somma delle shares è uguale alla share della somma.

12.3.1 Homomorphic property

Per lo schema di Shamir, ma anche per quello triviale, vale la homomorphic property: suppongo di avere un segreto S_F, genera un polinomio f(x). Un altro dealer genera un segreto S_g ed un polinomio g(x).
F da le 4 shares ai parties, e G fa lo stesso: F e G fanno riferimento allo stesso asse delle x (quindi le x date ai parties devono essere le stesse). Homomorphic property: la somma degli shares = share della somma. f(2) + g(2): f(x) + g(x) = (f+g)(2). Se devo aggregare i polinomi, dovrei dire quali sono i segreti, ma in questo modo non serve: ottengo la somma degli shares ma non ho informazioni sui segreti.

12.3.2 SMC

Computo il risultato di una funzione senza rivelare i dati in input.
Svariati casi d'uso

- Business/financial
- security medical: analisi del DNA senza che questo venga rivelato? Sì, field molto importante
- traffic monitoring

Molto underrated nel mondo reale, ma c'è dal 1982, ci sono anche ragioni storiche: le prime tecniche erano pesanti computazionalmente, ma ora ci sono tecniche efficienti.
Yao's millionair problem: decidere chi fra due persone è la più ricca. Potrebbero dire il loro patrimonio, ma così scopro un informazione in più. Possibile risolvere in problema con una disuguaglianza senza mostrare i valori. Problema è che l'approccio è molto pesante, usa oblivious transfer garbled circuits etc..., tecniche pesanti.
Dal 2010, ci sono diverse tecniche derivate dal SMC molto efficienti e pratiche. N parties P_1, P_2, ..., P_n ciascuno con valore z_i, computo la funzione f(z_1, z_2,...) tale che il risultato sia pubblico e non ci sian informazioni sui valori z_i. Si scopre che spesso la f è una funzione semplice, spesso è una somma. Se f è una somma pesata, che è molto frequente. si può risolvere in maniera molto efficiente, usando secret sharing schemes. Se restringo le funzioni a somme pesate, allora posso usare i secret sharing schemes e fare secure multipart computation: ogni input peer è un dealer, se ho una trusted third party, mando le z_i e questo le somma.
Ma ora posso creare uan trusted third party distribuita: diverse third parties untrusted la cui unica cosa che richiedo è che seguano il modello honest but curious, quindi so che il comportamento è onesto ma non ho garanzie sulla confidenzialità dei dati. Ho k peers, ogni peer ottiene lo share(z_i) e pubblica lo share del risultato. Quindi, il numero di input peers è almeno 3, altrimenti conoscendo il totale ed il mio dato, avrei il risultato. Il numero n di input peer spesso è grande, molto grande. I privacy peer k possono essere 2 se non

colludono, di più se ci sono collusioni. 2 è il numero ottimo, perché così posso usare schema (2,2), ma in principio posso usare ogni valore arbitrario t.
Se voglio fare operazioni su dei dati protetti: dovrei avere una third party fidata a cui affidare i dati (tramite canale sicuro), e che pubblicherà la somma dei valori. Con tecniche di secret sharing technique e SCM (che è un campo molto grande della matematica): se la tecnica di secret sharing ha la homomorphic property, i diversi peer fanno da dealer, creano le share per i loro segreti e mandano una share ad ogni privacy peer. Le operazioni di somma sono fatte su dati criptati, si combinano poi tutti i risultati pubblici.

12.3.3 Senza SMC: Third party

Tipicamente: molti input peers (1000+) ed un sotto-insieme di privacy peers k, di solito sono 2 ma anche 3 vanno bene.
Ma chi sono i privacy peers? Ci sono 5 peer che devono votare uno per l'altro e alla fine bisogna fare una somma. Si può risolvere chiamando due privacy peers, ma servirebbero altri due peer esterni. Si può risolvere senza privacy peer: posso usare i partecipanti stessi come privacy peer. Idea è invece di usare un (t,k) scheme, che è complesso, se decidiamo di usare uno schema (k, k) allora tutto si riduce ad un trivial secret sharing scheme. Non devo cambiare hardware o software, e le implementazioni non sono pesanti.
Devo creare sistema in cui ogni input peer agisce anche da privacy peer: ho 3 input peer i_1, i_2, i_3 e 3 privacy peer p_1, p_2, p_3. Quindi ogni peer contatta il privacy peer, in questo caso ogni peer da gli shares agli altri peer: $i_i = p_i$.
esempio: devo raccogliere soldi per un compleanno, senza far sapere quando mette il singolo peer. Decido un cap, e poi ogni peer genera la sua quantità, e due numeri random. Ogni peer quindi manda a se stesso il primo valore random, ad uno dei due peer il secondo numero random ed al terzo la differenza fra i 3 valori (il segreto - i due valori random), in tutto in *mod*. In parallelo, gli altri due parties fanno lo stesso. Quindi alla fine, ognuno ha le 3 shares: ora gli input peer agiscono come privacy peer, possono fare la somma e dopo aver fatto $mod(cap)$ ottengo lo stesso risultato che avrei sommando i segreti.

12.4 Verifiable Secret Sharing

Fin ora ho visto un modello di secret sharing "Honest but Curious", ovvero tutti i privacy peers operano onestamente ovvero danno la somma vera dei valori. Ma se i privacy peers sono malevoli, ovvero non seguono le regole? Servono quindi soluzioni per scoprire peer malevoli: shcemi di verifiable secret sharing.
Quindi le limitazioni del modello precedente è che sia i dealer che i privacy peers devono essere onesti, devo poter

- Verificare che lo share che il dealer mi ha dato sia corretto
- Poter verificare se gli share siano consistenti.

Primo schema: Feldman, schema crud ma ancora usato ogni tanto.
1991: schema di Pedersen, differenze rispetto a quello precedente.

12.4.1 Feldman scheme

Partiamo da un classico schema di Shamir (t,n), quindi il dealer genera il classico polinomio p(x), con p(0) = s. Distribuisce poi uno share a ciascuno dei parties (x_i, y_i).
Step aggiuntivo: il dealer prende un *modp* largo (ritorna il Dlog, prezzo da pagare), e per ogni coefficiente ed il segreto computa: $c_0 = g^s modp$, $c_1 = g^{a_1} modp$ etc... e li mette in chiaro. Rivela qualcosa? Bisognerebbe invertire $g^{a_i} modp$ e so che se p è grande, non è possibile invertire (in realtà ci saranno dei leak da queste informazioni). Queste operazioni sono dei commitments: non rivelo quali valori a_i uso, ma fornisco qualcosa per far si che dopo si possa verificare che ho usato veramente a_i; commitment = impegno.
Party i riceve lo share (x_i, y_i), dopo averlo rivelato, come fanno gli altri parties a verificare che y_i è corretto: bisogna verificare che $p(x_i) = y_i$. Il dealer mi ha potuto fornire lo share perché il dealer conosce p(x), ma i parties non lo conoscono, possono però fare il seguente trick: il party i rivela il suo share, ed un party si chiede se è corretto. Il dealer ha reso pubblici i commitment c_0,...,c_i: prendo c_0,c_1, e la x del party i. Quindi ora faccio $c_0 \cdot c_1^{x_i} \cdot c_2^{x_i^2} ... = (g^s) \cdot (g^{a_1})^{x_i} ... = g^s \cdot g^{a_1 x_i} ... = g^{s+a_1 x_i + a_2 x_i^2 \cdots} = g^{p(x_i)}$. La computazione può essere effettuata per chiunque, prima che la share sia rivelata. Ho effettuato una homomorphic computation $g^{p(x_i)} = g^{y_i}$, ma ora prendo la share y_i del party e ripeto la computazione, quindi se le cose non tornano c'è l'imbroglio.
esempio: polinomio di grado 2, prendo y_i, e controllo s $g^{y_i} = c_0 \cdot c_1^{x_i} \cdot c_2^{x_i^2}$, il tutto *modp*. Ma se computo il risultato non viene il segreto: le aritmetiche agli esponenti ed alle basi sono diverse, una è *modp* e l'altra è $\phi(p)$. Gli esponenti calano $mod\phi(p)$, non *modp*, che è un numero pari e quindi non si può usare Shamir.

12.4.2 Cos'è un commitment

In uno schema di comittment voglio impegnarmi di fare qualcosa dopo, ma inizialmente non voglio far sapere i valori che userò. 2 fasi

1. Ho un valore a segreto. Fase di commit: non mando il valore a, bensì una funzione di a, commit(a) che dovrebbe avere la hiding property, ovvero non rivelare nulla su a.

2. Fase 2, di reveal: vengono rivelate altre informazioni riguardo a, per poterne capire il valore.
   Quindi, siccome vedrò il valore solo dopo nel tempo, devo essere sicuro che non sia cambiato nel tempo. Ci deve essere una proprietà di binding tra il commitment ed il valore.

$c = g^x$ è un commitment per la x, questo è il Felman commitment. Un altro esempio è l'hash(x), perché se cambio x in x' avrei due digest diversi.
Ho due proprietà, una di hiding ed una di binding, per valutare un commitment scheme.

Felman: computationally hiding, se fornisco $g^x modp$, non è impossibile conoscere x, ma devo avere computing power sufficiente. È perfectly binding: faccio operazione in cui i numeri sono in range (0, p-1), mandando $g^x modp$, posso trovare un valore x + (p-1)k che mi da lo stesso valore di g^x, trovo quindi una collisione. Ma ora non posso trovare un altro x' nel range (0, p-1) tale che $g^x modp = g^{x+(p-1)k} modp$. Finché g è scelto bene, tutti i diversi valori di x danno un digest diverso, quindi perfect binding.
Come sarebbe una hash function come commitment? C'è computation hiding, ma è anche computation binding: selezionando due valori chi mi dice che non abbiano lo stesso hash? Quindi è il commitment peggiore, inoltre in Felman c'è homomorphic property mentre nell hash function no. Vorrei schema che fosse prefectly binding e perfectly hiding, che è impossibile ma almeno si può avere uno schema perfectly hiding e computationally binding.
Suppongo di usare *modp* largo, allora le a_i del polinomio p(x) sono scelte in un range(0, p-1) elevato. Ma il segreto s, in generale, non è un valore random perché dipende dall'applicazione. Se s è un età, avrà un certo range (es 1-120). Per dire che $g^x modp$ è una computazione sicura, devo avere che p è grande, ma anche x (altrimenti posso fare enumeration attack sulla x e testare a seconda dei valori, quale è = y_i). Quindi $g^s modp$ rivela informazioni sul segreto, che può essere abbastanza per rompere la sicurezza o no. Felman è computationally secure perché ha "solo" la hiding property.

12.4.3 Pedesrsen commitment

È perfectly hiding, ma computationally binding. Proprietà aggiuntiva di Pedersen è che homomorphic, voglio anche la perfectly hiding. Schema del 1991, usato anche in altri schemi (in cui è richiesta l'anonimità). Ci sono due valori g ed h, noti. Quando si fa commit del valore a, si usa anche una chiave r, random: $c = g^a \cdot h^r modp$, ho unito il segreto ad una chiave che è random (perso da un universo largo).Ora il valore a, piccolo, viene incrementato con il valore r e fare brute force è molto più complesso.Il commitment è homomorphic (vedi slides). Per ogni valore a' $\neq$ a posso trovare un valore unico r' tale che commit(a';r') = $g^{a'} h^{r'} = g^a h^r$ = commit(a;r). (vedi slides).
Si generano quindi due polinomi random, f(x) ed f'(x), in uno uso s e nell'altro r.
Ad ogni party si danno due share, y_i e z_i ciascuna corrispondente allo stesso x_i. Pubblico quindi i commitment:

- $c_0 = g^s h^r$
- $c_1 = g^{a_1} h^{b_1}$
- ...
- $c_{t-1} = g^{a_{t-1}} h^{b_{t-1}}$

È perfect hiding, inoltre nella verification riottengo $g^{y_i} h^{z_i}$. Meglio del computationally hiding, per il quale se il segreto s non è grande si può fare un dictonary

attack.
È sempre possibile risolvere l'uguaglianza c=$g^a h^r$, è possibile trovare una coppia $g^{a'} h^{r'}$ che può essere trovata ∀ a: quando rivelo il commit, ogni valore di a all'interno di c è equiprobabile e questa è la definizione della perfect secrecy. Ma se posso committare un qualunque altro valore allora il commitment non è binding? LO è, ma se ho sufficiente computing poweer posso risolvere l'equazione $g^a h^r = g^{a'} h^{r'}$, serve il $\log_g$(h) (è la trapdoor, che non è nota).
Dim: ho a, r è commit c = $g^a h^r$, più tardi voglio barare e dire che ho commitato con a'. Devo trovare r' tale che: $g^{a'} h^{r'} = g^a h^r$.
g ed h sono pubblici, diciamo che h = g^w, se g è un generatore del gruppo, posso prendere un qualunque altro punto ed esprimerlo come potenza di h. Quindi l'euazione diviene: $g^a g^{wr} = g^{a'} g^{wr'} = g^{a+wr} = g^{a'+wr'}$ = a + wr = a' + wr', ora le operazioni sono *modq*, p = 2q + 1 (voglio un gruppo primo per invertire l'equazione). Quindi r' = w^{-1} (a - a^{-1}+wr) (sono inversi modulari). Se conosco w, posso computare la verification key per un valore differente, devo risolvere un Dlog problem. È anche detto commitment con trapdoor, ovvero se conosco qualcosa in più il problema diventa facile.

12.5 Il gruppo moltiplicativo modulo p

Gruppo: coppia (G, ˚) con G un gruppo di elementi e ˚ operazione fra gli elementi del gruppo. Se l'operazione segue le 4 proprietà, G è un gruppo

- Chiusura: g_x = g_1 ˚ g_2 deve far parte del gruppo
- Esistenza del elemento neutro: un elemento I tale che g ˚ I = I ˚ g = g
- Inverso: ∀ g ∃ g^{-1} tale che g ˚ g^{-1} = I
- Associatività: ∀ g_1, g_2, g_3: (g_1 ˚ g_2) = g_1 ˚ (g_2 ˚ g_3)

Può esserci anche la proprietà commutativa, se c'è il gruppo si dice anche Abeliano

12.5.1 Il gruppo Zp*

Z = interi, p = prime, *= moltiplicativo.
Gruppo formato dai p-1 elementi (con p primo) = {1,2,3,...,p-1}. È un gruppo finito, e se considero come operazione la moltiplicazione *modp* è un gruppo Abeliano.
Proprietà dei gruppi tutte rispettate, l'inverso? L'insieme garantisce sempre un inverso quando: ∀ x, se GCD(x,N) = 1 allora x ha invero *modN*. Nel caso di N primo, tutti gli elementi hanno un inverso (0 non è un elemento del gruppo).
Exponentiation: sembra una nuova operazione, ma è la ripetizione dell'unica operazione del gruppo, per k volte. x^k = x ˚ x ˚ x... (k volte). Per il gruppo Z_p^*, esiste un generatore del gruppo di ordine m, g tale che: {g^0, g^1,...} = tutti gli m del gruppo.
Ordine del gruppo: la massima iterazione prima di tornare all'inizio. Se il

gruppo ha p-1 elementi, l'ordine massimo è di p-1. Un prime order group è un gruppo in cui se m è primo, ogni membro è un generatore. Nel caso di Z_p^*, questo non è un prime order group, perché m è un numero pari (è = p-1, e p è primo).
esempio: $Z_1 1^*$, quali membri sono generatori? g = 2 è un generatore per $Z_1 1^*$. Se g = 3, ottengo solo un sotto-insieme degli elementi, così detto sotto-gruppo di ordine 5 (5 elementi nel sotto-gruppo).
A seconda di h, in alcuni casi posso avere tutti gli elementi del gruppo, in altri casi solo un sotto-insieme.
Quindi: o g genera tutto il gruppo, oppure ricade in un sotto-gruppo, e tutti i gruppi sono periodici.

12.5.2 Strong primes

p = 83, l'ordine del gruppo $g^x mdop$ = p-1, ovvero 82 che non può essere primo. Ovvero, p-1 = 2·(), ma ora fra tutti i possibili primi, è possibile trovarne uno in cui 2 + moltiplicato per un certo numero q, primo? Questi numeri sono detti strong primes: p = 2q + 1, così che p-1 = 2q, con q primo.
83: 83-1 = 82 = 2·41, conseguenza: nel caso peggiore di generatore, ricado in un sotto-gruppo di taglia $\frac{p-1}{2}$, in questo caso 41. Quindi ogni membro x:

- Genera l'intero gruppo, oppure
- Genera un sotto-gruppo di ordine q

Se p e q sono grandi, i due gruppi che genero sono entrambi grandi (implicazione importante, ad esempio per DH). In RSA, si usano p e q strong primes, così che N = p·q, $\phi(N)$ = (p-1)·(q-1), che in generale se p = 2·p' + 1 e q = 2·q' + 1, avrò $\phi(N)$ = 4·p'·q'.

12.5.3 Quadratic residue subgroup

Per Z_p^*, diciamo che x è un residuo quadratico se ammette radice quadrata, ovvero esiste un a tale che: $a^2 modp$ = x. Teorema: non tutti i punti ammetto radice quadrata. C'è un modo semplice per fare il check su un x:
$x^{\frac{p-1}{2}}$ ha due possibili valori, o è 1 o è -1, ovvero vedi il valore in posizione $\frac{p-1}{2}$, o è 1 o è -1. Se prendo un valore x, e ne faccio il quadrato e poi *modp* e questo mi da 1, ottengo un QR e so che generano un sub-group (simboli di Legendre), il sub group sarà ordine nell'ordine di q.
Felman: il problema dello schema è che la matematica di g_i^y è $mod(p-1)$, ma se scelgo g come QR, ovvero come generatore del sub-group e se scelgo p come strong prime, posso avere ad esponente della g aritmetica $mod\frac{p-1}{2}$, quindi lavoro di nuovo su un numero primo q, quindi posso lavorare con base *modp*, e se g è un QR, l'esponente è *modq*. Quindi ora, con queste assunzioni, il Felman scheme funziona con Shamir *modq*.

12.6 Distributed Key Generation

Voglio generare un valore pubblico $g^x modp$, che nasconde un valore privato corrispondente x, ad esempio x è la chiave usata in public key encryption schemes, basati su Dlog. Solitamente, si parte da x e poi si computa $g^x modp$, ma questo vuol dire che conosco x all'inizio. È possibile avere uno schema alla fine del quale ho una chiave pubblica h, nota da tutti e nessuno conosce x, ma se serve ricostruire x si può? Problema risolto nel 1991 (sempre da Pedersen), ci sono crypto systems basati su Dlog, basati sul fatto che x è privato e $g^x modp$ è pubblico. Schema in cui nessuno conosce x e tutti $g^x modp$ è utile per molte applicazioni, ad esempio non ci interessa la chiave privata, che viene ricostruita solo quando necessario.
Schemi di Distributed Key Generation, si possono usare in contesto in cui non servono trusted third parties.
Esempio: genero $g^x modp$ tra 4 parties, così che queste collaborino per generare la chiave pubblica ma se uno dei party esce, 3/4 possono ricostruire la chiave privata (schema (3,4)).
Ogni party ha $a_{0,i}$ ed il segreto sarà $s = a_{0,1} + a_{0,2} + a_{0,3} + a_{0,4}$ (ogni $a_{0,i}$ sarà generato random). Inoltre, ogni party genera polinomio di grado t-1, dove viene nascosto il segreto che ha generato. Ogni party fa da dealer: ad esempio $p_1(x) = a_{0,1} + a_{1,1}x + a_{2,1}x^2$. Ora ogni party da agli altri 3 il suo share, ogni party avrà uno share del polinomio degli altri 3.
Quindi, come $party_1$, prendo la somma degli shares e computo y_1 = somma dei miei shares: $p_1(1) + p_2(1) + p_3(1) + p_4(1)$. Ora, posso rendere pubblici i commitment dei segreti degli shares, $g^{a_{0,i}}$.
Ho creato un polinomio, che è la somma dei singoli polinomi, in cui il segreto non è noto. Nono solo tutti hanno implicitamente s, ma è possibile rendere pubblico il commitment per s.
Quindi, tutti conoscono g^s, nessuno conosce s, ma se necessario tutti hanno uno share di s quindi se 3/4 decidono di ricostruire s, c'è la trapdoor.

12.7 Threshold and policy-based cryptography

Una serie di applicazioni pratiche del secret sharing, in cui non è necessario avere delle trusted party.
esempio: Bitcoin, problema: per usarlo, serve private key, per firmare la transazione. Chi controlla la private key? Entra nel gioco lo shared secret, threshold crypto: 3 attori. Uno è il wallet, professional service, alcuni danno la chiave alla compagnia che tengono traccia della chiave (es Coinbase) ma c'è una trusted third party. Se non mi fido: 2/3 sharing scheme, multisig 2/3 in gergo Bitcoin. Metto chiave USB in cassaforte, ci sono io e Coinbase, dico che la signature può essere fatta se ci sono 2 parties. Creo uno schema in cui do 3 shares: uno a me, una sulla USB, una su Coinbase. Voglio fare buy/sell: uso il mio share e quello di Coinbase, mediante tecniche di threshold signatures, che mi permettono di fare signature senza ricostruire la chiave.
Ma cosa succede se Coinbase prende e scappa: hanno solo uno share, ma io

posso spendere i soldi perché posso ricostruire la chiave integrando lo share nella cassaforte col mio. Mentre, cosa accade se qualcuno si frega il PC? Nulla, perché posso ricostruire la chiave tramite gli Share di Coinbase e della cassaforte. (Bitcoin non usa quello che vedremo).

12.7.1 Threshold encryption-case study ElGamal

ElGamal encryption scheme, uno dei più importanti insieme a DH ed RSA. ElGamal:

- Asymmetric crypto scheme, usato per fare public key encryption
- Basato su Dlog, molto più conveniente per EC points (curve ellittiche). Ispirato da DH, basato su una interpretazione di DH. DH scheme viene reso un cipher asimmetrico
- È un cipher probabilistico, prezzo da pagare è che non si può trasmettere un singolo valore bensì due. Es: se plaintext = 2048 bit, il ciphertext = 4096 bit.

Sketch: ho un primo largo p, un generatore del gruppo g, chiave privata s e chiave pubblica h = $g^s modp$, inoltre c'è un valore r random, che viene generata ogni volta che voglio spedire qualcosa.
Se devo mandare qualcosa a qualcuno: chiedo la sua pub key, che uso per cifrare il mio messaggio. Ora, la chiave pubblica è $g^s modp$, devo criptare un messaggio: encrypt : (R, c) = (g^r, $m \cdot h^r$). Perché funziona: g^r e random, m è il messaggio che è moltiplicato per una quantità random, quindi è ancora random (o meglio, è derivata da una quantità random). Come funziona la decryption: m = c· R^{-s}, non posso dividere c per h^r, è stata computata dal sender, che non mi ha dato r. Ma $h^r = (g^s)^r$, questo è = g^{rs}, è la classica idea di DH. Decrypta quindi $\frac{m \cdot g^{rs}}{g^{rs}}$, quindi inverto dividendo per g^{rs}, ed ottengo quindi m. Nessuno può computare: s ce l'ha solo il receiver, g^r ce l'ha solo il sender, e lo trasmette per far si che il receiver possa ricostruire il messaggio m.
Questo è lo schema Vanilla, bisogna migliorarlo per poterlo usare nel mondo reale, es: posso fare H(h^r) = keystream $\oplus$ m.
Threshold manner: posso fare threshold encyption? Ovvero, posso criptare qualcosa per un gruppo di persone, così che se qualcosa è da solo non può decriptare, ma se ci sono t parties si può? È la threshold encryption: per accedere ad alcuni dati, servono almeno 3 autorità che devono scambiarsi qualcosa. Serve applicare il secret sharing: posso dare le shares di s ai vari parties, ma nella ricostruzione della chiave privata s per fare decryption, ognuno potrà decriptare i messaggi seguenti. Quindi l'approccio funzionerebbe una sola volta, dopo aver ricostruito il segreto: game over.
Non bisognerebbe ricostruire s, ma solo quello che serve per decriptare quello specifico messaggio: posso riuscirci, garantendo la confidenzialità dei messaggi precedenti?
esempio: cifro il messaggio m_1: (g^{r_1}, m_1, h^{r_1}), avrò che m_2 = (g^{r_2}, m_2, h^{r_2}), cambia la quantità r, che nessuno ha. Se ricostruisco $g^{r_1 s}$, posso decifrare solo il

primo messaggio. Devo ricostruire il segreto all'esponente: Pedersen, Feldman commitments.
Suppongo che s sia data da un dealer (può anche essere un DKG), ognuno avrà le shares di s, se devo ricostruire s, dovrei sommare le shares per le Λ, i coefficienti di Lagrange (Shamir classico). Posso farlo all'esponente? Se moltiplico termini esponenziali, è come fare la somma degli esponenti. Quindi

- Ognuno ha lo share di s, devono decifrare il messaggio
- Prendono il messaggio g^r, mh^r, ognuno computa il Λ coefficient
- Ogni party prende g^r e fa: $((g^r)^{share})^{\Lambda_{party//glialtridue}}$

Quindi si moltiplicano questi termini nel punto 3, per ottenere g^{rs} e per poter decriptare il messaggio, nessuno ha conoscenza del segreto s (viene ricostruito all'esponente).

12.7.2 Parantesi: ECDH

Perché viene abbandonato RSA: in TLS DH ti permette di avere PFS (principale ragione per cui RSA è stato abbandonato), ma anche perché DLOG cryptosystems sono molto utili quando si lavora su curve ellittiche: RSA non sarebbe conveniente come altre tecniche. La ragione delle EC: maggiore scalabilità: ci sono chiavi più piccole, ma non è questo il motivo per l'uso delle curve ellittiche, bensì è dovuto al symmetric key equivalent: si misura la taglia delle chiavi per un avere la stessa sicurezza di un determinato cipher (es AES-128): nel caso di RSA il monudlo è di 3072 bit, mentre EC di 283. Ma nel caso di una chiave di 256 bit: 15360 bit di RSA modulo, 571 bit per EC. RSA non scala linearmente con la dimensione della chiave di AES, mentre nel caso delle curve ellittiche si scala di un fattore 2. Per questo conviene usare EC, ma per farlo è molto più conveniente usare gruppi di ordine primo.

12.7.3 Asymmetric ciphers: "hybrid" usage

Non si usa sempre TLS per trasferire i dati: devo setuppare una connessione fra client e server, ma se devo mandare una mail in maniera asincrona? Preparo la mail, la cirfo con la chiave privata del mio recevier e gliela mando. 2 problemi: se il messaggio è lungo, devo splittare il messaggio in chunks, in RSA ogni chunk è limitato (ricorda PKCS#1, c'è il padding). Problemi: devi applicare l'encryption a tutti i blocchi e devo poterli linkare fra loro, RSA usa 4-5 OOM più della symmetric encryption dal punto di vista della computazione. Soluzione è hybrid encyption: prendo il messaggio, genero questa chiave k random e cifro il messaggio usando la chiave k, uso un asymmetric encryption per cifrare la chiave k. Quindi il messaggio sarà criptato usando la chiave k, con cipher simmetrico, mentre la chiave sarà cifrata con asymmetric encryption. Molto più veloce, usa i vantaggi di symmetric encryption. La chiave sarà sicuramente più piccola di 1024 bit ad esempio, quindi consisterà di un blocco solo.

12.7.4 ElGamal-like crypto: ECIES in 5G

Hybrid encyption in 5G, ma le compagnie più forti e grandi di solito usano Hardware Security Modules. IN hardware ancora non del tutto supportato, in software sì, da molte librerie.
Usato per cifrare l'identità dell'IMSI (ma è ancora attaccabile, downgrades). Approccio: Elliptic Curve Integrated Encryption Scheme (ECIES), schema molto tecnico. Vediamo una versione senza elliptic curves, schema clean:

- Ho la SIM card, dove è hardcoded la chiave pubblica del mio operatore g^{HN}. non c'è bisogno di recuperarla dalla rete, quindi non serve certificato
- Quando voglio generare qualcosa, genero una quantità effimera g^x. Ho x, g^x e g^{HN}. Cosa posso fare: cifrare la chiave simmetrica k, ma la cosa è più sottile.Invece di generare k e poi cifrarla, l'approccio è di combinare i due termini: k = HKDF($g^{(HNx)}$), ottiene chiavi di encryption ed integrity (ricorda che c'è il counter qui). Non è ElGamal, ma ricorda qualcosa.
- Uso AES_K(SUPI), ma anche HMAC. Si poteva usare AEAD in 5G, invece hanno scelto di fare encrypt then MAC. Quindi mando all'operatore il messaggio (g^x, ENC_K(MSG), HMAC'_K(MSG)). Operatore prende la sua chiave privata, fa $(g^x)^{HN}$, dove HN è la chiave privata e da qui deriva le chiavi con HKDF per poter decifrare e fare HMAC.

12.7.5 Threshold signature

Il problema sembra il duale: siamo un gruppo di persone e vogliamo firmare un messaggio in modo che solo se siamo in t(su n) è possibile fare questa firma. Una qualunque insieme di t persone in un gruppo di n può firmare un messaggio, se ci sono meno di t persone deve essere impossibile firmare un messaggio.
Si dovrebbero riusare gli approcci di signature già esistenti, non vorrei che la size esploda al crescere di t.
Ho due primi grandi p e q, genero ϕ(N) = (p-1)(q-1), genero e e d. Voglio firmare m: ne faccio l'hash, elevo alla d, per verificare elevo alla e e controllo l'hash (tutto modN).
Con threshold: prendo d, genero il polinomio f(x) = d + a_1x +..., gli shares saranno (x_i, y_i) modϕ(N). Per la signature: $\text{H(m)}_i^y \Lambda_{x_i} \text{modN}$, lo fa ogni membro del gruppo, una volta computati, si mettono insieme e si ritorna a H(m)^d.
C'è un problema: ongi party prende H(m), lo eleva alla y_i, per farlo serve solo conoscere N, poi lo eleva alla Λ_i e anche qui server conoscere solo N. Sembra che vada tutto bene, ma: ho p, ho q (strong primes), ho n = p·q, ricavo il polinomio f(x) e genero 3 shares del polinomio. Firmo il messaggio m, quindi mi computo la signature: ma invece ottengo un errore: i lambda non sono interi, li ho computati senza il modular inverse, ma non posso farlo perché serve ϕ(N) e i parties non ce l'hanno. La consegna degli shares viene fatta dal dealer, che conosce ϕ(N), mentre la computazione deve essere fatta dai parties che non solo non conoscono ϕ(N), non possono proprio. Servono gli inversi per poter

implementare la signature, ma al sicurezza di RSA risiede nel fatto che gli inversi non possono essere computati senza conoscere ϕ(N), che si ottiene con la fattorizzazione e quindi si rompe RSA.
Come evitare gli inversi: bisognerebbe restringere le x_i in modo da var si che i Λ siano tutti interi, ma questo è un incubo.
Victor Shoup: assumo di usare i classici x_i, ho L players massimi, mi concentro sul Lagrange denominator, usando il worst case dell'interpolazione di tutti e gli L shares, che sicuramente divide i!(L-i)!, questo è il worst case. Coefficiente binomiale $\frac{(L)}{(i)}$ è un intero per definizione, quindi i!(L-i)! è un divisore del coefficiente binomiale, ottengo quindi L!.
Quindi se prendo $\Lambda_i(x) \cdot L!$, ottengo un intero, lavoro su questo termine $L_i^{'}(x)$. Ma siccome questo valore è un intero, posso dare l'operazione $H(m)^{y_i \cdot \Lambda'_{x_i}}$, quindi ho un nuovo schema:

- Ogni party computa $H(m)_i^y \Lambda'_1$ etc...
- Ora, facendo il prodotto delle computazioni ottengo $H(m)^{d \cdot L!}$, tranne per un fattore che posso cancellare.

Per togliere L!: devo avere l'inverso di L! mod ϕ(N), sono tornato al punto di partenza. In RSA: attacco del common modulus, supponiamo di fare il seguente errore. In RSA, una volta computato N ho un grande effort che si fa una volta. Quindi perché non riusare lo stesso N e generare diverse encryption keys e_a ed e_b, che do ad Alice ed a Bob. Alice cripta m ed anche Bob per caso cripta lo stesso messaggio. m^{e_a} ed m^{e_b}, ma le due chiavi d sono diverse. In realtà, se vedo due encryption dello stesso messaggio con due chiavi diverse, decifrarlo (sotto certe condizioni, ovvero le due chiavi e devono essere coprime). Algoritmo di eulcide esteso: lo applico ad $e_a r + se_b$ e cerco i due s ed r. Conosco le chiavi pubbliche, determino r ed s, prendo $(m^{e_a})^r$ e applico all'altro s, li moltiplico: $m^{e_a r + e_b s} = m^1$. Quindi, il modulo non di riusa MAI.
Quindi, voglio ricostruire la mia digital signature, i parties hanno una share della private key e vogliamo firmare senza ricostruire d. Prendiamo $H(m)_i^y \Lambda_i L!$ e poi moltiplichiamo tutto insieme. Ora ho $(H(m)^d)^L!$, come togliere L!, se avessi $(H(m)^d)^{(altro)}$ avrei la possibilità di fare common module attack. Ho $(H(m)^d)^e$, che è H(m), quindi se e ed L! sono coprimi, posso ricavare la mia signature iniziale. Quindi y = H(m), ho $y^{L!} = y^{\Delta}$ ed y^e, quindi trovati r ed s applico l'attacco e derivo la firma, sono entrambi modN. Unico compromesso: prendere una chiave pubblica e che sia primo e più grande di L, in quanto L! = 1234...L, quindi se e > L non avrà fattori comuni con L! Abbiamo quindi una signature standard con un key sharing standard.
Ulteriori note:

- La computazione è fatta sul sottogruppo dei residui quadratici
- Nel paper di Shoup ci sono anche verificabilità e prove di sicurezza

Problema è che serve un dealer: come generare share di una chiave privata d? Deve conoscere N e ϕ(N), quindi può rompere il sistema. C'è un paper francese

(grr) che mostra come si può usare Pedersen per generare strong primes, quindi per generare RSA terms in maniera distribuita.

12.8 Mobile devices resilient to capture

MacKenzie & Reiter, 2003. Sviluppo di sistemi non triviali in cui si usa principio del "divide et impera" (in termini di mantenimento di informazione crittografiche). Problema: ho un terminale mobile, qualcuno lo ruba e non voglio che ne abbia accesso (oggi ci sono soluzioni proprietarie).
1 laptop rubato ogni 12 secondi (dato del 2010):

- Sondaggio su 329 organizzazioni, 86400 laptop rubati, valore di circa 2.1 mld$
- Valore dei dati è più importante del laptop in se

Oggi si usano ransomware: encryptin dei dati e chiedono dei soldi per avere la decifratura (con un backup li fotti).

12.8.1 Capture resilient device

Un device che non può essere usato da nessuno al di fuori dell'owner del device. es: per accedere ad un PC, ho bisogno di una crypto key, come faccio a proteggerla?

- Soluzione classica è metterla in un tamper-proof hardware, ma questo è un po' un macello, poi device può essere tampered se c'è tempo
- Si potrebbe lockare con una password, ma questa può essere tentata con dictonary attack.
- Ottengo una chiave dalla rete, ma anche qui c'è un problema in quanto il repository in rete deve essere sicura.

Soluzione del 2003: combina questi 3 ingredienti, user + device + network, in maniera intelligente. Assunzione: il device è connesso quando usato, la soluzione prevede di usare un "capture-protection server" nella rete, quindi va contattato per accedere ai dati. Il main goal era di non trustare il c-p server. 2 approcci:

- Basic one: usano standard crypto, ma in maniera intelligente
- Approccio esteso: usa uno schema (2,2) per secret sharing.

3 party scenario:

- User, che è l'unico che conosce la password
- Device, con secret key e public key, ha del materiale segreto
- Server, con pub e private keys.

Diversi scenari di attacco:

- La password viene scoperta
- Il device viene rubato, non è tumper-proof
- Il server viene crackato, non è trusted. Il server che non è trusted non è per via del fatto che sia malevolo, semplicemente non ci fidiamo del fatto che nessuno possa crackare il server, il livello di sicurezza non mi convince (es delphi).

Questi attacchi non sono singoli, questo era il problema: per essere resiliente devo esserlo ad ogni coppia degli attacchi (se tutti e 3 insieme = game over, non si sono più trusted anchors, a meno di introdurre altro).
Soluzione di base: robusti a

- Server and password known: attacker non può fare sign/decrypt
- Device cracked/stolen: solo dictonary attack online
- Device and server craked: attacker può solo fare offline dictonary attack.

Non potevano essere resilienti a device and password cracked.
La soluzione di base usa solo crypto completamente standard.

12.8.2 Tickets

Assunzione: il device ha accesso alla rete. Idea: c'è una singola chiave da qualche parte nel device e se questa è protetta, i dati del PC sono protetti. Idea è proteggere il PC così da cifrare la chiave, quando l'utente accede questa chiave è decifrata cooperando con la rete.
Quindi: PC ha la chiave per accedere ai dati cifrata, l'utente ha la password ma questa non basta a decifrare la chiave, deve collaborare col server per poterlo fare.
Soluzione:
Device initialization: quando compro il device, devo fare queste operazioni:

- L'utente decide una password, salvata temporaneamente sul device (in chiaro), poi verrà cancellata dal sistema; ottengo anche la public key del server
- Genero una coppia di chiavi (pub, pr) del device
- Genero una chiave random V, che sarà persistente.
- Genero una chiave a persistente
- Faccio hash della password: b = H(P)
- Cripto la chiave segreta: $SK_{device} \oplus PRF(v; P)$. Uso uno stream cipher, il keystream è generato usando come crypto key V e come seme la password.

- Per poter decifrare il device bisogna conoscere sia il valore V, che è salvato nel device, ma anche la password P che è nota solo all'utente(serve computare il keystream)
- Creazione del ticket: tkt = $E_{pk-server}$[a, b, c]
- Ora cancello dal sistema P, b, c, e la SK de device.
- Cosa rimane: un ladro trova nel device v, e la PK del device. La SK del device è stata cifrata nel messaggio ticket, usando la pub key del server, quindi solo il server può decifrare. Ma se anche il server decifra, le informazioni rimangono protette: ottengo H(P) e $SK_{device} \oplus$ PRF(v; P).

Key retrieval: questa fase è online, voglio attivare il device

- L'utente inserisce la password, quindi il device può computare β = H(P).
- Manda al server il tiket, insieme all'hash della password cifrata con la chiave pubblica del server.
- Il server apre il ticket, decifra il messaggio e controlla che b = β, b è l'hash della vera password (quello che di solito si trova in un DB). IL server vuole controllare che l'utente sia autentico e quindi possegga la password. È la fase di user authentication
- Se l'utente è autentico, il server ritorna c = $SK_{device} \oplus$ PRF(v; P)
- Utente mette in XOR con col keystream (ha P e v, quindi può ricostruirlo) e ottiene SK_{device}.

Key retrieval vero:

- L'utente, oltre che computare β, computa anche ρ, random e che servirà come chiave random per poter ottenere c. Così, non serve che la rete sia sicura
- Come faccio ad essere sicuro che il messaggio sia generato davvero dal device? Genero una chiave random a, authentication key (qualcosa che si usa in un HMAC), che preinstallo nel device, è symmetric authentication, ma è usata in maniera asimmetrica. Per garantire che il messaggio sia autentico, faccio $HMAC_a$[tkt, $E_{pk-server}$[β, ρ]].
- Il server ha la chiave a, se qualcuno ha modificato il valore di a il server se ne rende conto. Il server trova a nel tiket, quindi non serve nemmeno che se la salvi. Può quindi, dopo aver decifrato il ticket, controllare che l'HMAC sia valido. Quindi così posso autenticare il device.
- Server quindi dopo la decryption ha β e ρ, può autenticare anche l'utente, ed ora può rimandare indietro il messaggio
- Il messaggio rimandato è $\rho \oplus$ c, senza necessità di avere un encryption protocol (hanno dimostrato la sicurezza di questi steps).

12.8.3 Attacchi

Possibili attacchi:

- Il server viene crackato e la passoword viene scoperta: la chiave v è nel device, è ancora segreta. Sono un attacker, conosco p e posso anche controllare il server. Quindi, posso decodificare il ticket: conosco a, b ma c è stata cifrata con SK_{device} e con PRF(v; P), ma v non è nota, è comunque cifrata nel device.
- Device viene rubato: ho l'authentication key a. Ma per decifrare il device, ho bisogno della password dell'utente e di v: v ce l'ho, am non ho P, posso provare a crackarla: il check che β = b viene fatto online, quindi dictonary attack viene fatto online (servono in media 1M di richieste), ma a questo punto avrò tecniche per riconoscere i tentativi multipli.
  L'hash della password è salvata in un DB, non sta nel server remoto, quindi anche avendo accesso al server non si trova l'hash della password.
- Device + server craked: attacker manda l'HMAC al server, il server è controllato da lui quindi può decifrare il ticket ed ottenere a, b e c, quindi può ottenere hash(password), c'è protezione ma solo dal fatto che va fatto un dictonary attack offline.

Ci sono delle limitazioni: se rubo device + password, game over. Ora è possibile far girare il protocollo in maniera corretta.
Si può fare meglio: secret sharing, non viene mai rivelata la chiave SK, nemmeno allo stesso device. Posso usare un device per firmare una transazione senza dirgli la chiave? Sì, threshold sigtaure.

12.8.4 Secret sharing (2,2) per RSA

Non confondere con Victor Shoup, lì bisognava gestire esponenti fratti, qui usiamo uno schema (2,2): d private key, e public key. Lo share 1 sarà d_1 random, share 2 è d_2 = d - d_1, tutto è fatto $mod\phi(N)$. Ho solo quantità intere, nessuna complicazione. Voglio firmare il messaggio: uso entrambe le shares: $H(m)^{d_1} \cdot H(m)^{d_2} = H(m)^{d_1+d-d_1} = H(m)^d mod N$. Altra motivazione per cui è importante dimenticarsi di Shamir secret sharing quando si può usare uno schema triviale (n,n).
Protocol2: initialization

- Password P, PK del server, pub key del device (N,e) e pr key d (ed anche $\phi(N)$).
- Genero v, a come prima
- Generazione dello $share_1$: l'ideale sarebbe generare una quantità random ed un'altra a partire da questa. Ma nessuno dice che non si può generare d_1 pseudo-random: genero d_1 = PRF(v;P). È pseudo-random, che può essere riprodotto conoscendo 2 cose, la chiave del device v e la password P.

- Genero share$_2$ come d$_2$ = d - d$_1$ $mod\phi(N)$
- Genero poi l'hash della password, ed il ticket che conterrà [a, b, d$_2$, N], non contiene più la chiave segreta d, ma solo uno dei due shares.

Key retrieval: bitcoin use case, voglio firmare una transazione (in bitcoin si usa ECDSA, farla con la threshold richiede un hell of the work).

- User inserisce la password, manda HMAC$_a$[tkt, E$_{pk-server}$[H(m), β, ρ]], includo anche l'hash del messaggio.
- Server non sa chi sono, apre il ticket, controlla il message authentication, decifra il messaggio, autentica l'utente (β = b ?)
- Manda il messaggio come $\rho \oplus H(m)^{d_2} modN$. Il messaggio non è mai in chiaro, c'è privacy preserve.
- User ottiene $H(m)^{d_2}$ e deve moltiplicare con $H(m)^{d_1}$, ma d_1 è computabile, quindi per ogni signature chiedo aiuto al network server, ma questo non consocerà mai d.

d non è mai in chiaro, se l'attacker controlla la password ed il device, non può più ottenere la chiave segreta d. Se il server non è informato del furto, continuerà a rispondere ed a firmare transazioni, ma la secret key non è nota. Disabling key t: il server può essere bloccato per far si che non risponda più alle send. Se blocco le transazioni, l'attacker non può più fare transazioni, la chiave d non è nota. Introdotta una chiave t apposita, inclusa nel ticket, finché ho un backup della chiave t posso dire al server di bloccare il device mandandogli t. Ora, il server può controllare che u non è in un DB che contiene tutti i device bloccati (es u = H(t), salva quello nel DB).