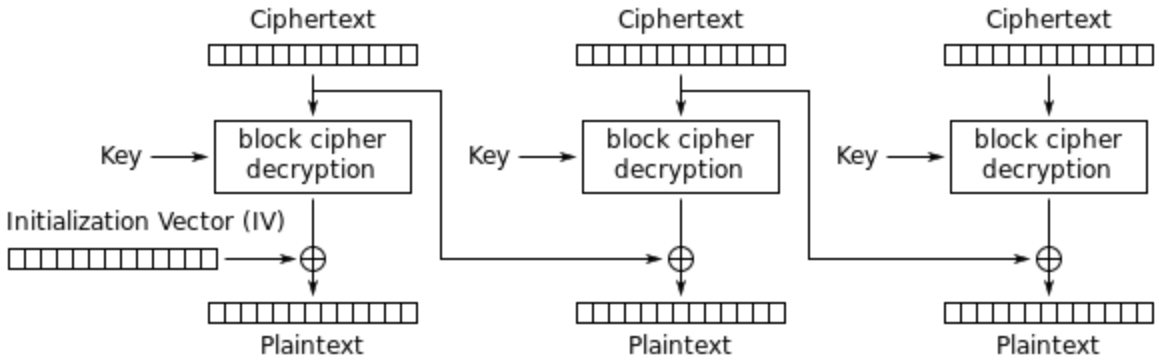
1. TLS - (Transport Layer Security) - rozwinięcie protokołu SSL (Secure Socket Layer). Zapewnia on szyfrowanie danych, monitorowanie ich integralności, oraz uwierzytelnianie serwera. Schemat działania (TLS handshake) :
   - wysłanie przez klienta informacji o obsługiwanej wersji SSL, dozwolone sposoby szyfrowania i kompresji
   - serwer odpowiada podobnie tj. Wysyła wybraną wersję protokołu i sposób szyfrowania i kompresji, a następnie wysyła swój certyfikat i informacje o swoim kluczu publicznym
   - klient wysyła klucz sesji zaszyfrowany za pomocą klucza publicznego serwera i powiadamia, że może przełączyć się na komunikację szyfrowaną
   - serwer informuje o wykonaniu poleceń i też powiadamia o przełączeniu się na komunikację szyfrowaną.
   - Handshake
2. SSH - Secure Shell, standard protokołów komunikacyjnych wykorzystywany w sieciach TCP/IP, następca Telnet. Transfer wszelkich danych jest zaszyfrowany oraz możliwe jest rozpoznanie użytkownika na wiele sposobów. Najczęściej stosowany sposób szyfrowania to AES
3. 2FA - 2 Factor Authentication - system zabezpieczeń polegający na potrzebie posiadania dodatkowej informacji podczas logowania oprócz hasła (np. Kodu otrzymanego przez tel.) zabezpiecza przed wszelkimi wyciekami prywatnych informacji czy niektórymi atakami typu phishing.
4. Application Specific Password - hasło które system może przydzielić aplikacji, aby ułatwić jej logowanie i umożliwić korzystanie tylko z tej funkcji z jakiej musi. Problem z tym u Google polegał na tym, że mając takie hasło można było zrobić dowolną rzecz na koncie ofiary, podszywając się pod aplikacje.
5. IV - Initialization vector - ciąg znaków, który zależnie od specyfikacji systemu bezpieczeństwa, zapewnia dodatkowe bezpieczeństwo obok klucza. Musi być losowe lub pseudolosowe.

6. CBC -Cipher Block Chaining



Cipher Block Chaining (CBC) mode decryption

7. Szyfry strumieniowe-algorytm symetryczny, który szyfruje oddzielnie każdy bit wiadomości. Algorytm ten składa się z generatora strumienia bitowego, będącego kluczem szyfrującym oraz elementu dodającego (na przykład operacji XOR).
8. AES-Advanced Encryption Standard- symetryczny szyfr blokowy, który traktuje blok jako macierz (stan).

Rozszerzenie klucza – z głównego klucza algorytmu "tworzy się" kolejne klucze. AES wymaga osobnego klucza 128-bitowego dla każdej rundy, plus jeden dodatkowy.

runda wstępna

Dodawanie klucza rundy – każdy bajt macierzy stanu jest mieszany z blokiem rundy za pomocą operatora bitowego XOR.

Rundy

Zamiana Bajtów – nieliniowa zamiana, podczas której każdy bajt jest zamieniany innym.

Zamiana Wierszy – etap transpozycji, podczas którego trzy ostatnie wiersze macierzy stanu są cyklicznie zmieniane określoną ilość razy.

Mieszanie Kolumn – Operacja odnosi się do kolumn macierzy. Polega na łączeniu czterech bajtów w każdej kolumnie.

Dodaj klucz rundy

Final Round (brak operacji Mieszania Kolumn)

Zamiana Bajtów

Zamiana Wierszy
Dodaj klucz rundy.

9. Certificate pinning

Polega na pominięciu hierarchii certyfikatów (CAcert->Cert1->Cert2) wydawanych przez CA (patrz 13.), a dodaniu własnego/nie potwierdzonego certyfikatu do potwierdzonych certyfikatów.

10. Extended Validation dla SSL - rozszerzony certyfikat X.509 potwierdzający osobowość prawną. Uzyskanie takiego certyfikatu wymaga weryfikacji osobowości przez CA (wymagane jest spełnienie większej ilości kryteriów). Przeglądarki wyświetlają obok kłódki nazwę na którą został wydany certyfikat
11. CRL - Certificate revocation list - lista certyfikatów, wydawana przez CA, które mimo ważnej daty certyfikatu nie są bezpieczne.
12. OCSP - Online Certificate Status Protocol - protokół służący do uzyskiwania listy certyfikatów X.509, które przestały być zaufane przez CA (patrz 13.)
13. CA- Certificate authority - zaufany podmiot który wystawia certyfikaty
14. Downgrade attacks TLS - atak polegający na stosowaniu starszych zabezpieczeń kompatybilnych z nowszymi, ale mogącymi posiadać wady. Podatność na ten atak wykryto np. w OpenSSL, gdzie podczas negocjacji atakujący mógł wymusić starszą wersję TLS. Metodami ochrony przed tym atakiem jest usuwanie kompatybilności wstecznej.
15. HSTS - mechanizm bezpieczeństwa sieci, który chroni strony przed atakami takimi, jak wymuszone zmniejszenie poziomu protokołu czy też przechwycenie sesji. Dzięki niemu możemy do serwerów połączyć się tylko za pomocą HTTPS.
16. DSA - Digital Signature Algorithm - asymetryczny algorytm do szyfrowania

    Generowanie klucza:

    -Wybieramy funkcję hashującą, oraz długości L i N (L>N)

    -Wybieramy N-bitową liczbę pierwszą q

-Wybieramy L-bitową liczbę pierwszą p, taką, że p - 1 jest wielokrotnością liczby q
-Wybieramy g, którego rząd mod p jest równy q
-Przekazujemy(p,q,g) pomiędzy użytkowników systemu
-Użytkownik wybiera sekret x; 0< x < q
-Oblicza klucz publiczny $y = g^x mod\ p$
Podpisywanie:
- niech H - funkcja hashująca, m wiadomość
- generujemy losowe k ; 1 < k < q
- $r = (g^k mod\ p)\ mod\ q$
- jeżeli r = 0 to wybierz inne k
- $s = k^{-1}(H(m) + xr)\ mod\ q$
- jeżeli s = 0 to wybierz inne k
- Podpisem jest para (r,s)
Weryfikacja:
- sprawdzamy czy 0 < r < q i 0 < s < q
- jeżeli tak to $w = s^{-1}\ mod\ q$
- $u_1 = H(m) * w\ mod\ q$
- $u_2 = r * w\ mod\ q$
- $v = (g^{u_1} * y^{u_2} mod\ p)\ mod\ q$
- podpis jest prawidłowy jeżeli $v = r$

17. RSA - Rivest–Shamir–Adleman -

Sposób działania:
N- liczba składająca się z 2 liczb pierwszych n=pq
E- klucz publiczny (N, e)
D - klucz prywatny (N, d)
d można wyliczyć z wzoru:
$d \equiv e^{-1}\ mod\ NWW(p,q)$
Enc:
$c \equiv m^{\ e}\ mod\ n$
Dec:
$c^d \equiv (m^e)^d\ mod\ n \equiv m\ mod\ n$

18. Self-signed certificate certyfikat podpisany przez ten sam podmiot, który się nie posługuje.
19. Phishing - atak polegający na wyłudzeniu informacji przez podszywanie się pod podmiot, który tych informacji mógłby wymagać, np. do logowania
20. Skipfish - program, który szuka potencjalnych wektorów ataku na podanej stronie. Wektory są generowane na podstawie ataków słownikowych i site crawl (przejścia po wszystkich możliwych podstronach)
21. SQL injection - atak polegający na nadużywaniu informacji wstawianych do kwerendy, z jakiegoś pola lub requesta (GET), aby wyświetlić/zmienić/usunąć dane z bazy danych.
    Przykład:
    ‘ OR 1=1 ‘
    ‘; DROPDATABSE XYZ; --
22. XSS - Cross-site scripting - polega na umieszczeniu na stronie skryptu, który może wykonywać niepożądane czynności na innej stronie do których atakujący nie ma dostępu.
23. XSRF - Cross-site request forgery- atak polegający wykonywaniu komend do których atakujący nie ma dostępu przez użytkownika, który owe komendy może wykonać, ale w chwili ataku nie robi tego celowo. Np. wysłanie komuś linku, który po kliknięciu zmieni hasło osobie zalogoanej.
24. Blind signatures - forma podpisu cyfrowego, w której wiadomość jest maskowana zanim zostanie podpisana. Dzięki temu podpis może być weryfikowany tak jak zwykły cyfrowy podpis.
    Schemat:
    - losujemy r względnie pierwsze z N
    - $m' = mr^e \mod N$
    - $s' = (m')^d \mod N$
    - $s = s' * r^{-1} \mod N$
    - to działa dzięki temu że $r^{ed} = r \mod N$

- $s = s' * r^{-1} = (m')^d r^{-1} = m^d r^{ed} r^{-1} = m^d \, mod \, N$

25. Constant time - wykorzystywane jako ochrona przeciwko timing attack, polegająca na tym, że nie zależnie od długości danych, obliczenia są wykonywane w stałym czasie (wait nie załatwia sprawy, musi się coś liczyć)
26. Timing Attack - atak polegający na analizowaniu czasu wykonywania algorytmu, poprzez próbowanie różnych danych wejściowych. Zapobiega się poprzez tworzenie implementacji algorytmów, które są wykonywane w stałym czasie.
27. Captcha- Completely Automated Public Turing test to tell Computers and Humans Apart - system polegający na rozróżnianiu człowieka od bota. Używany np. przy wysyłaniu zapytań do serwera, które ze swojej natury są drogie, a wykonywane w nadmiernej ilości mogą spowolnić pracę/wyłączyć serwer
28. Logowanie przez zewnętrzny serwis - np. Google, polega na zrzuceniu na zewnętrzny, zaufany system ciężaru logowania i otrzymywania od danego serwisu tokena który zawiera tylko część danych, na które się wcześniej umówiliśmy. Np. Aplikacja ChatApp prosi tylko o e-mail, nazwę użytkownika i avatar i tylko takie dane otrzymuje.
29. Safe primes - $q = 2p + 1$ liczby pierwsze mniej podatne na faktoryzację
30. Przepełnienie buffora - stuacja w której buffor/ miejsce przeznaczone na dane jest przepełnione i nadpisuje pozostałą pamięć. Można wykorzystać do ataku na podatny system, aby wydobyć wartości z pamięci.
31. Key store - jest to miejsce w którym trzymamy certyfikaty albo klucze publiczne i odpowiadające im prywatne używane np. Przy OpenSSL.
32. Intel SGX - Software Guard Extensions to rozszerzenie, które umożliwia stworzenie przestrzeni chronionej w pamięci systemowej. Działanie SGX polega na tym, że zamiast identyfikować i izolować

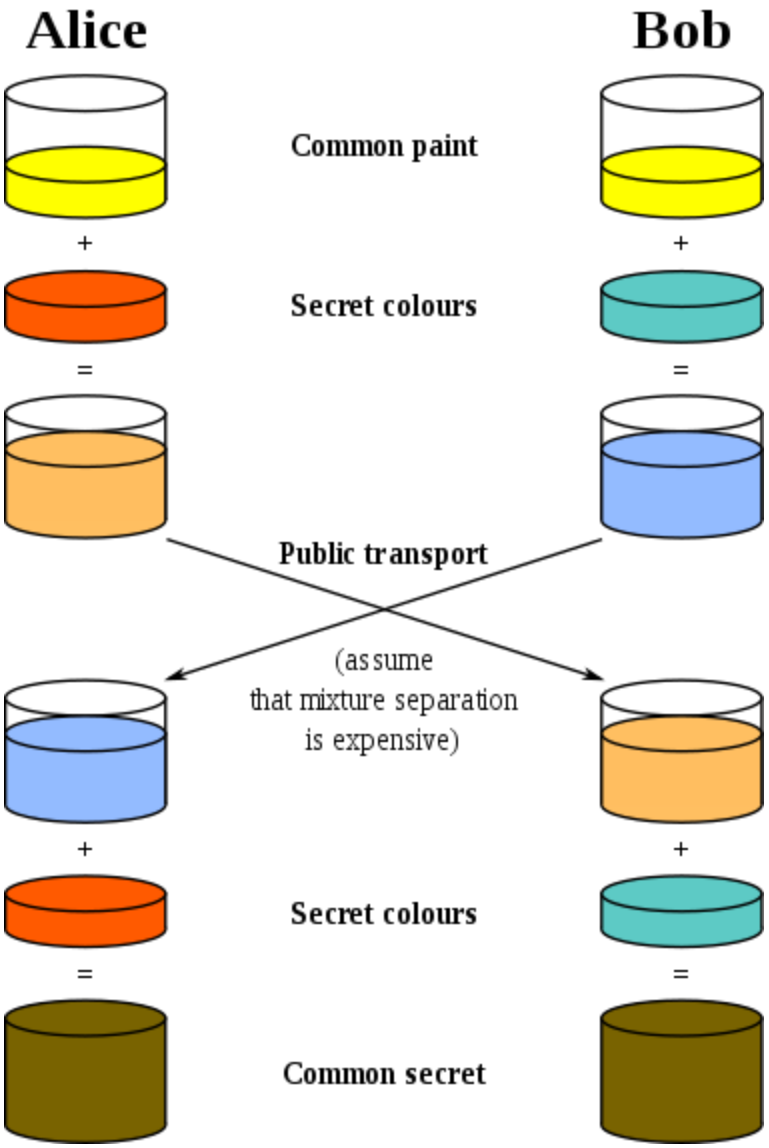
złośliwe oprogramowanie, zamyka najważniejsze dane i kod we wspomnianej przestrzeni i blokuje do nich dostęp. Wtedy to poziom uprawnień szkodliwej aplikacji nie ma znaczenia.

33. Polityka bezpieczeństwa

Polityka bezpieczeństwa informacji to dokument opisujący pewne założenia przyjęte w firmie dotyczące zabezpieczenia informacji. Polityka bezpieczeństwa nie jest pojęciem jednoznacznym, możemy mieć bowiem do czynienia z:

a. Polityką bezpieczeństwa całościową,
b. Polityką bezpieczeństwa w rozumieniu Ustawy o Ochronie Danych Osobowych
c. Polityką bezpieczeństwa opisującą założenia tylko dla wybranego systemu IT (zbioru danych).

34. Protokół Diffie-Helmanc-Jego siła oparta jest na trudności obliczenia logarytmów dyskretnych w ciałach skończonych. Klucz uzgodniony za pomocą tego algorytmu może zostać wykorzystany do szyfrowania komunikacji. Algorytm pozwala bezpiecznie uzgodnić klucz nawet jeżeli istnieje osoba, która podsłuchuje proces uzgadniania klucza, nie chroni jednak przed atakami typu man in the middle. Algorytm nie nadaje się do szyfrowania i deszyfrowania wiadomości.



35. ElGamal - to jeden z dwóch najważniejszych algorytmów kryptografii asymetrycznej (obok RSA). System jest oparty na trudności problemu logarytmu dyskretnego w ciele liczb całkowitych modulo duża liczba pierwsza.

Generowanie klucza:

1<k<p

α - dowolny generator grupy

$\beta = \alpha^k \ mod \ p$

Szyfrowanie:

x -losowa liczba

$(\alpha^x \ (mod\ p)\ ,\ m \times \beta^x (mod\ p))$

Deszyfrowanie:

$\alpha^{xk}\ mod\ p\ \equiv \alpha^{kx}\ mod\ p\ \equiv\ \alpha^{k^x}\ mod\ p\ \equiv\ \beta^x\ mod\ p$

Następnie liczymy γ z rozszerzonego Euklidesa:

$\gamma\beta^x\ +\ \delta p\ = 1$

$\gamma\beta^x\ \equiv 1\ mod\ p$

$\gamma = (\beta^x)^{-1}\ mod\ p$

$(m \times \beta^x) \times \gamma \equiv m \times (\beta^x \times \gamma) \equiv m \times 1 \equiv m \mod p$

Podpis cyfrowy:

$y = \alpha^r$ (mod p)

$s = (H(m) - ky)r^{-1}$ mod p-1 gdzie H to funkcja haszująca

Aby sprawdzić:

$\beta^y y^s = \alpha^{H(m)}$

Dla prawidłowego będzie zachodzić:

$\alpha^{ky}\alpha^{rs} = \alpha^{H(m)}$

$\alpha^{ky+r\left((H(m)-ky)r^{-1}\right)} = \alpha^{H(m)}$

$\alpha^{ky+H(m)-ky} = \alpha^{H(m)}$

$\alpha^{H(m)} = \alpha^{H(m)}$

Jeżeli r jest znane to można uzyskać d

$y^{-1}\ (H(m) - sr) = y^{-1}\ \left(H(m) - (H(m) - ky)r^{-1}r\right) = y^{-1}ky = k$

36. PKI - zbiór osób, polityk, procedur i systemów komputerowych niezbędnych do świadczenia usług, uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego, prywatnego i certyfikatów elektronicznych. W szczególności jest to szeroko pojęty kryptosystem, w skład którego wchodzą CA, urzędy rejestracyjne, użytkownicy, oprogramowanie i sprzęt. Najpopularniejszym standardem jest X.509
37. Shell injection polega na takim wprowadzeniu danych, aby zmienić działanie programu. Zachodzą kiedy niesprawdzony kod trafia do interpretera.

38. Ballon hashing - to funkcja hashująca hasło, która jest skomplikowana pamięciowo do obliczenia, z powodu wielu wykonywanych hashowań hashy, przez co złamanie go oznacza wielki koszt pamięciowy do zapamiętania każdej iteracji hasha aż do N następnie, wybieramy losowe hashe jeszcze je hashujemy. Ostatecznym hashem jest hash znajdujący się na N-tej pozycji
39. Side channel attacks - są to ataki opierające się na informacjach uzyskanych z fizycznej implementacji, a nie ze słabości algorytmu. Np. czas, pobór energii, dźwięk czy przecieki elektromagnetyczne
40. Secure Multiparty-computation (dziedzina) - celem tego jest stworzenie takiej metody, w której kilku uczestników może przekazywać dane i otrzymać publiczny wynik, ale żadne z uczestników nie zna odpowiedzi innych uczestników. W tej sytuacji warto zauważyć, że potencjalny atakujący kontroluje uczestników, zamiast podsłuchiwania.
41. Secure function evaluation (rozwiązywanie funkcji w 40.) polega na rozwiązaniu sytuacji w której mamy funkcję i uczestników i chcemy aby przekazać każdemu użytkownikowi wynik funkcji, ale aby nie znał danych od innych użytkowników.