Bezpieczeństwo systemów informatycznych

dr Marek Miśkiewicz

2021

POLSKO-JAPOŃSKA AKADEMIA TECHNIK KOMPUTEROWYCH

mmiskiewicz@pjwstk.edu.pl

Dysk p:

/public/mmiskiewicz/BSI

Egzamin w formie testu (wielokrotnego wyboru)
na podstawie materiału prezentowanego na wykładach

Literatura

- William Stalling - „Bezpieczeństwo systemów informatycznych. Zasady i praktyka”, Helion 2019
- William Stallings - **Network Security Essentials: Applications and Standards**, Pearson 2011
- William Stallings - **Cryptography and Network Security Principles and Practice**, Pearson 2017
- Simson Garfinkel, Alan Schwartz, Gene Spafford - **Practical Unix & Internet Security**, O’Reilly 2003
- Janusz Stokłosa, Tomasz Bilski, Tadeusz Pankowski - **Bezpieczeństwo danych w systemach informatycznych**, Wydawnistwo Naukowe PWN, Warszawa–Poznań 2001.
- A. J. Menezes, P. C. van Oorschot, S. A. Vanstone - **Kryptografia stosowana**, WNT, Warszawa, 2005
- Michał Szychowiak - **Bezpieczeństwo systemów komputerowych**, http://wazniak.mimuw.edu.pl

RFC 2828 definiuje **informację** jako "fakty i idee, które mogą być reprezentowane (zakodowane) jako różne formy **danych**", a dane jako "informacje w określonej fizycznej reprezentacji, zwykle jako sekwencje symboli, które mają określone znaczenie; w szczególności dane, które mogą być przetwarzane lub produkowane przez komputer. "

RFC (ang. Request for Comments – dosłownie: prośba o komentarze) – zbiór technicznych oraz organizacyjnych dokumentów mających formę memorandum związanych z Internetem oraz sieciami komputerowymi. Każdy z nich ma przypisany unikatowy numer identyfikacyjny, zwykle używany przy wszelkich odniesieniach. Publikacją RFC zajmuje się Internet Engineering Task Force.

„Wszystko jest informacją”

Informacja jest zasobem

Zasoby posiadają określoną wartość

Ochrona zasobów leży bezpośrednio w interesie podmiotu który jest ich właścicielem lub jest niezbędna do realizowania wyznaczonych celów.

Dane jako fizyczna reprezentacja informacji powinny i muszą być chronione.

Bezpieczeństwo (bezpieczeństwo komputerowe)

Ochrona zapewniona przez zautomatyzowany system informatyczny w celu osiągnięcia i zachowania **integralności**, **dostępności** i **poufności** **zasobów** systemu informatycznego (w tym sprzętu, oprogramowania, oprogramowania wewnętrznego, informacji / danych i telekomunikacji).

Poufność
Confidentiality

- Zapewnia, że prywatne lub poufne informacje nie są udostępniane lub ujawniane nieuprawnionym osobom (poufność danych).

- Zapewnia, że osoby kontrolują lub wpływają na to, jakie informacje z nimi związane mogą być gromadzone i przechowywane oraz przez kogo i komu można je ujawnić (prywatność).

- **NIST:** Zachowanie autoryzowanych ograniczeń dostępu do informacji i ich ujawniania, w tym środków ochrony prywatności i informacji zastrzeżonych. Utrata poufności to nieuprawnione ujawnienie informacji.

Integralność
Integrity

- Dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany (integralność danych).

- System realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub nie (integralność systemu).

- **NIST:** Ochrona przed niewłaściwym rozpowszechnianiem lub zniszczeniem informacji, w tym zapewnienie niezaprzeczalności i autentyczności informacji. Utrata integralności to nieautoryzowana modyfikacja lub zniszczenie informacji.

Dostępność
Availability

- Właściwość bycia dostępnym do wykorzystania na żądanie w założonym czasie przez kogoś lub coś, kto lub co ma do tego prawo.

- **NIST:** Zapewnienie terminowego i niezawodnego dostępu do informacji i ich wykorzystywania. Utrata dostępności jest zakłóceniem dostępu lub możliwości korzystania z informacji lub systemu informatycznego.

Autentyczność
Authenticity

- Tożsamość podmiotu lub zasobu jest taka jak deklarowana; dotyczy użytkowników, procesów, systemów lub instytucji.

- Właściwość bycia prawdziwym, zdolnym do weryfikacji i zaufania (trusted); zaufanie co do poprawności (validity) transmisji i jej źródła. Oznacza to także weryfikację, czy użytkownicy są tymi, za kogo się podają.

Rozliczalność
Accountability

- Właściwość zapewniająca, że działania podmiotu mogą być jednoznacznie przypisane tylko temu podmiotowi.

- Rozliczalność umożliwia niezaprzeczalność, „odstraszanie”, izolację błędów, wykrywanie włamań i zapobieganie im.

Niezaprzeczalność
Non-repudiation

- brak możliwości wyparcia się, ochrona przed fałszywym zaprzeczeniem
- przez nadawcę faktu wysłania danych
- przez odbiorcę faktu otrzymania danych

Identyfikacja
Identification

- możliwość rozróżnienia użytkowników, np. użytkownicy w systemie operacyjnym są identyfikowani za pomocą UID (ang. user identifier)

Uwierzytelnianie
Authentication

- proces weryfikacji tożsamości użytkownika. Najczęściej opiera się na tym:
  - co użytkownik wie (knowledge factor),
  - co użytkownik ma (ownership factor),
  - kim lub czym użytkownik jest (inherence factor)

Autoryzacja
Authorization

- proces przydzielania użytkownikowi praw dostępu do zasobów

Kontrola dostępu
Access Control

- system składający się z urządzeń, oprogramowania i procedur organizacyjnych, mający na celu identyfikację podmiotu i nadzorowanie przestrzegania praw dostępu do zasobów

Information Security

Internet Security

Network Security

Computer and Software Security

???

Information Security

Internet Security

Network Security

Computer and Software Security

CZŁOWIEK

Bezpieczeństwo systemów informacyjnych
Computer Security

- Narzędzia kryptograficzne
- Kontrola dostępu
- Bezpieczeństwo baz danych i zasobów w chmurze
- Złośliwe oprogramowanie
- Ataki „Denial-of-Service”
- Systemy IDS (Intrusion Detection Systems)
- Ściany ogniowe i systemy IPS (Intrusion Prevention Systems)

Bezpieczeństwo systemów informacyjnych
Software Security and Trusted Systems

- Ataki typu „Buffer Overflow”
- Bezpieczeństwo aplikacji
- Bezpieczeństwo systemów operacyjnych
- Bezpieczeństwo wielopoziomowe i „Trusted Computing”

Bezpieczeństwo systemów informacyjnych
Risk Management

- Zarządzanie bezpieczeństwem i ryzykiem
- Polityka bezpieczeństwa
- Bezpieczeństwo infrastruktury i zasobów
- Bezpieczeństwo „zasobów ludzkich”
- Audyty bezpieczeństwa

Bezpieczeństwo systemów informacyjnych
Network Security

- Protokoły i standardy bezpieczeństwa sieci
- Uwierzytelnianie w sieci (PKI)
- Bezpieczeństwo sieci WiFi

Jak można inaczej rozumieć bezpieczeństwo?

System komputerowy jest **bezpieczny** gdy:

- użytkownik może na nim polegać,
- oprogramowanie działa zgodnie ze specyfikacją.

Dane wprowadzane do systemu:

- zachowują swoje atrybuty (wystarczające),
- nie są tracone,
- nie są modyfikowane w niekontrolowany sposób,
- nie zostaną pozyskane przez nieuprawniony podmiot.

Bezpieczeństwo a wiarygodność

System komputerowy jest **wiarygodny** gdy jest:

- bezpieczny (secure) - zapewnia ochronę danych,
- bezpieczny (safe) - nie stwarza zagrożeń dla otoczenia,
- dostępny (available) - działa ma bieżąco,
- niezawodny (reliable) - odporny na ataki i awarie

AGRESOR/ATAKUJĄCY

- osoba świadomie podejmująca atak na system informatyczny/informacyjny w celu uzyskania korzyści
- kraker (ang. cracker), intruz, włamywacz, napastnik, wandal, przestępca.

Typy ataków

- **PASYWNY** - atakujący ma dostęp do danych (także w kanale komunikacyjnym) - może je czytać, ale ich nie modyfikuje
- **AKTYWNY** - atakujący modyfikuje dane lub je preparuje
- **MAN IN THE MIDDLE** - atakujący przechwytuje dane w kanale komunikacyjnym

Typy ataków

- **LOKALNY** - Zainicjowany przez podmiot znajdujący się na granicy bezpieczeństwa ("osoba wewnętrzna"). Osoba posiadająca informacje poufne jest upoważniona do dostępu do zasobów systemowych, ale wykorzystuje je w sposób niezatwierdzony przez tych, którzy udzielili jej zezwolenia.

- **ZDALNY** - Zainicjowany „z zewnątrz” przez nieautoryzowanego lub nieuprawnionego użytkownika systemu ("outsider"). W Internecie potencjalni zewnętrzni napastnicy to amatorzy dowcipnisie, zorganizowani przestępcy, międzynarodowi terroryści i wrogie rządy.

Formy ataków

- **EAVESDROPPING** - podsłuch, najczęściej analiza ruchu sieciowego.
- **REPLAYING** - odtwarzanie, atakujący używa ponownie zebranych wcześniej danych.
- **MASQUERADING** - podszywanie się, atakujący daje zaufany lub uwierzytelniony podmiot.
- **TAMPERING** - manipulacja, akt celowego modyfikowania (niszczenia, manipulowania lub edytowania) danych przez nieautoryzowane kanały.
- **EXPLOITING** - atakujący posługuje się wiedzą o znanym błędzie w oprogramowaniu lub gotowym narzędziem wykorzystującym taki błąd.

Fazy ataku

1. Skanowanie – szukanie słabości, np. sondowanie usług
2. Wyznaczenie celu, np. niezabezpieczona usługa, znany exploit
3. Atak na system
4. Modyfikacja systemu umożliwiająca późniejszy powrót
5. Usuwanie śladów
6. Propagacja ataku

Przestępstwa związane z bezpieczeństwem

- włamanie do systemu komputerowego,
- nieuprawnione pozyskanie informacji,
- destrukcja danych i programów,
- sabotaż (sparaliżowanie pracy) systemu,
- piractwo komputerowe, kradzież oprogramowania,
- oszustwo komputerowe i fałszerstwo komputerowe,
- szpiegostwo komputerowe.

Według ekspertów Rady Europy przestępstwa komputerowe dzielą się na grupy:

- oszustwo związane z wykorzystaniem komputera,
- fałszerstwo komputerowe,
- zniszczenie danych lub programów komputerowych,
- sabotaż komputerowy,
- obrażanie innych osób w sieci
- „wejście” do systemu komputerowego przez osobę nieuprawnioną (patrz: cracking, haker),
- „podsłuch” komputerowy,
- bezprawne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych,
- bezprawne kopiowanie topografii półprzewodników,
- podszywanie się pod inne osoby lub pod firmy
- modyfikacja danych lub programów komputerowych,
- szpiegostwo komputerowe,
- używanie komputera bez zezwolenia,
- używanie prawnie chronionego programu komputerowego bez upoważnienia,
- metoda salami.

Obszary w których prawnie wymagana jest ochrona danych i informacji

Prawo dotyczące ochrony danych odobowych	Prawo oświatowe	Prawo bankowe	Prawo finansowe
Prawo przemysłowe	Prawo archiwalne	Prawo dotyczące informatyzacji państwa	Prawo telekomunika-cyjne
Prawo dotyczące statystyki publicznej	Prawo autorskie	Prawo z zakresu ochrony zdrowia	?

Wybrane akty prawne wymagające bezpieczeństwa informacyjnego

Ustawa o ochronie danych osobowych

Ustawa o ochroni informacji niejawnych

Ustawa o podpisie elektronicznym

Ustawa o świadczeniu usług drogą elektroniczną

Ustawa o finansach publicznych

Ustawa o rachunkowości

Ustawa o dostępie do informacji publicznej

Ustawa o systemie informacji oświatowej

Ustawa o narodowym zasobie archiwalnym i archiwach

Ustawa o prawie autorskim i prawach pokrewnych

Kodeks karny - Rozdział XXXIII kodeksu dotyczy przestępstw przeciwko ochronie informacji

Prawo

- **Art. 267.** §1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- §2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.
- §3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.
- §4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.

Prawo

- **Art. 268.** §1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- §2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.
- §3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
- §4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.

Prawo

- **Art. 269. §1.** Kto, na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
- §2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji.

Prawo

- Art. 287. §1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
- §2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
- §3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Prawo → nakazuje nam zrobienie czegoś

Normy → jak należy to zrobić

Rodzina norm

ISO/IEC 270XX

ISO/IEC 27000:2018	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
ISO/IEC 27001:2013	Information technology -- Security techniques -- Information security management systems -- Requirements
PN-EN ISO/IEC 27001:2017-06	Technika informatyczna — Techniki bezpieczeństwa — Systemy zarządzania bezpieczeństwem informacji — Wymagania
ISO/IEC 27002:2013	Information technology -- Security techniques -- Code of practice for information security controls
PN-EN ISO/IEC 27002:2017-06	Technika informatyczna — Techniki bezpieczeństwa — Praktyczne zasady zabezpieczania informacji
SO/IEC 27003:2017	Information technology -- Security techniques -- Information security management systems -- Guidance
ISO/IEC 27004:2016	Information security management — Monitoring, measurement, analysis and evaluation
PN-ISO/IEC 27004:2017-07	Technika informatyczna — Techniki bezpieczeństwa — Zarządzanie bezpieczeństwem informacji — Monitorowanie, pomiary, analiza i ocena
ISO/IEC 27005:2011	Information technology -- Security techniques -- Information security risk management
PN-ISO/IEC 27005:2014-01	Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji

ISO/IEC 27006:2015	Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems
PN-ISO/IEC 27006:2016-12	Technika informatyczna -- Techniki bezpieczeństwa -- Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji
ISO/IEC 27007:2017	Information technology -- Security techniques -- Guidelines for information security management systems auditing
PN-ISO/IEC 27013:2014-01	Technika informatyczna -- Techniki bezpieczeństwa -- Wytyczne do zintegrowanego wdrożenia ISO/IEC 27001 oraz ISO/IEC 20000-1
PN-ISO/IEC 27017:2017-07	Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze
ISO/IEC 27032:2012	Information technology -- Security techniques -- Guidelines for cybersecurity

www.pkn.pl
www.iso.org

Common Criteria

Międzynarodowa norma Common Criteria (CC) definiuje kryteria oceny bezpieczeństwa systemów teleinformatycznych.

Standard ISO/IEC 15408 Common Criteria for Information Security Evaluation (Wspólne kryteria do oceny zabezpieczeń informatycznych) składa się z trzech części:

- ISO/IEC 15408-1 (CC Part 1) zawiera: wprowadzenie, opis modelu zarządzania ryzykiem i kreowania uzasadnionego zaufania oraz struktur podstawowych dokumentów, opracowywanych na potrzeby certyfikacji produktu lub systemu;
- ISO/IEC 15408-2 (CC Part 2) zawiera katalog komponentów funkcjonalnych (ang. functional components) służących do modelowania funkcjonalnych wymagań bezpieczeństwa;
- ISO/IEC 15408-3 (CC Part 3) zawiera katalog komponentów uzasadniających zaufanie (ang. assurance components), służących do modelowania wymagań uzasadniających zaufanie do funkcji zabezpieczających.

Common Criteria

Common Criteria zaleca stosowanie rygorystycznych wymagań dla procesów rozwoju, produkcji i utrzymania produktów IT po to, aby użytkownicy mogli mieć pewność, że stosowane w tych produktach zabezpieczenia są poprawne i efektywne. Zaufanie do produktu jest dodatkowo potwierdzane w drodze niezależnej oceny i certyfikacji wykonywanych przez akredytowane laboratoria i instytucje.

PN-ISO/IEC 15408-1:2016-10	Technika informatyczna -- Techniki bezpieczeństwa -- Kryteria oceny zabezpieczeń informatycznych -- Część 1: Wprowadzenie i model ogólny
PN-ISO/IEC 15408-2:2016-10	Technika informatyczna -- Techniki bezpieczeństwa -- Kryteria oceny zabezpieczeń informatycznych -- Część 2: Komponenty funkcjonalne zabezpieczeń
PN-ISO/IEC 15408-3:2016-10	Technika informatyczna -- Techniki bezpieczeństwa -- Kryteria oceny zabezpieczeń informatycznych -- Część 3: Komponenty uzasadnienia zaufania do zabezpieczeń

Orange Book
Trusted Computer System Evaluation Criteria

Dokument powstały z inicjatywy Agencji Bezpieczeństwa Narodowego Departamentu Obrony USA (**NSA DoD**) oraz Narodowego Biura Standaryzacji (**NIST**). Wydany w 1983 roku w postaci **pomarańczowej książeczki**, której zawdzięcza swoją nieoficjalną nazwę. Dokument ten opisuje podstawowe wymagania jakie muszą spełnić środki ochrony w systemie komputerowym do przetwarzania informacji podlegającej ochronie. Dokument został zaktualizowany w roku 1985 a następnie zastąpiony przez międzynarodowy standard **Common Criteria**.

Orange Book
Trusted Computer System Evaluation Criteria

Dokument koncentruje się na sposobach zapewnienia poufności informacji i wyróżnia 4 poziomy kryteriów:

D1 — C1 C2 — B1 B2 B3 — A1

Orange Book
Trusted Computer System Evaluation Criteria

D1

Ochrona minimalna (ang. Minimal Protection)
Obejmuje systemy, które posiadają jedynie **fizyczną ochronę przed dostępem**. W systemach tej klasy, każdy kto posiada fizyczny dostęp do komputera, ma nieskrępowany dostęp do wszystkich jego zasobów. Przykładem systemu tej klasy jest komputer IBM PC z systemem MS-DOS bez zabezpieczeń hasłowych.

Orange Book
Trusted Computer System Evaluation Criteria

C1

Ochrona uznaniowa (ang. Discretionary Protection)
Zapewnia elementarne bezpieczeństwo użytkownikom pracującym w środowisku wieloużytkownikowym i przetwarzającym dane o jednakowym poziomie tajności. Systemy C1 stosują **sprzętowe lub programowe mechanizmy identyfikacji i upoważniania użytkowników**. System zabezpiecza dane identyfikacyjne i hasła przed niepowołanym dostępem. Identyfikacja użytkowników powinna być wykorzystywana w każdym trybie dostępu do zasobu. Każdy użytkownik ma pełną kontrolę nad obiektami, które stanowią jego własność. **Większość systemów unixowych zalicza się do tej klasy.**

Orange Book
Trusted Computer System Evaluation Criteria

C2

Ochrona z kontrola dostępu (ang. Controled Access Protection). Udostępnia prowadzenie dla każdego użytkownika indywidualnie **dziennika zdarzeń**, związanych z bezpieczeństwem oraz środki do określania zakresu rejestrowanych zdarzeń (podsystem Audit). Systemy tej klasy posiadają **rejestrację zdarzeń i rozszerzoną identyfikację użytkowników**. Poziom C2 stawia też dodatkowe wymagania dotyczące szyfrowania haseł, które muszą być ukryte w systemie (niedostępne dla zwykłych użytkowników).

Orange Book
Trusted Computer System Evaluation Criteria

B1

Ochrona z etykietowaniem (ang. Labeled Security Protection). Pierwszy z poziomów wprowadzający różne stopnie tajności (np. "tajne", "poufne" itp.). W systemach tej klasy stosuje się **etykiety określające stopień tajności** dla podmiotów (procesów, użytkowników) i przedmiotów (plików). Zezwolenie na dostęp do danych zapisanych w pliku udzielane jest podmiotom **na podstawie analizy etykiet**. Opatrzone etykietami procesy, pliki oraz urządzenia zawierają pełny opis stopnia tajności obiektu oraz jego kategorii.

Orange Book
Trusted Computer System Evaluation Criteria

B2

Ochrona strukturalna (ang. Structured Protection).
Określa wymagania, sprowadzające się do takich elementów, jak: etykietowanie każdego obiektu w systemie, **strukturalna, sformalizowana polityka ochrony systemu**, przeprowadzenie **testów penetracyjnych** dla wykrycia ewentualnych "dziur" w modelu. Uprawnienia do zmian pełnomocnictw w zakresie dostępu do obiektów są zastrzeżone dla autoryzowanych użytkowników. Nie ma możliwości odzyskania skasowanych informacji.

Orange Book
Trusted Computer System Evaluation Criteria

B3

Ochrona przez podział (ang. Security Domains).
Wymusza **izolację** pewnych dziedzin (obszarów). Części systemu istotne ze względu na bezpieczeństwo przetwarzania powinny być oddalone od części zapewniających użytkownikowi pewne użyteczne dla niego funkcje, ale niemające związku z bezpieczeństwem przetwarzania. Mechanizmy zarządzania pamięcią chronią daną dziedzinę przed dostępem lub modyfikacją ze strony oprogramowania funkcjonującego w innej dziedzinie. Tworzona jest **wielowarstwowa struktura abstrakcyjnych, odseparowanych wzajemnie maszyn z wydzielonymi prawami ochrony**. Nadzorowaniu w zakresie spełnienia wymagań podlega również proces projektowania systemu.

Orange Book
Trusted Computer System Evaluation Criteria

A1

Konstrukcja zweryfikowana (ang. Verified Design)
Wymaga formalnego **matematycznego dowodu** poprawności modelu bezpieczeństwa, jak również formalnej specyfikacji systemu i bezpiecznej dystrybucji. Jak dotąd, bardzo niewiele systemów uzyskało certyfikat tego poziomu.

Nie ma czegoś takiego jak absolutne bezpieczeństwo.

Bezpieczeństwo jest zawsze związane z ekonomią.

Utrzymuj poziom wszystkich zabezpieczeń na tym samym poziomie.

Atakujący nie będzie „przedzierał się” przez zabezpieczenia, będzie je obchodził.

Stosuj zabezpieczenia wielopoziomowe.

Nie należy polegać na bezpieczeństwie opartym na „zaciemnianiu”

Nie należy dawać osobie lub programowi większych uprawnień niż są im potrzebne do wykonania zadania.

Bezpieczeństwo powinno być integralnym elementem projektu.

Program lub protokół jest uważany za „niebezpieczny” dopóty dopóki jego bezpieczeństwo ie zostanie dowiedzione.

Bezpieczeństwo to kompromis z wygodą.

Keep it simple

Bezpieczeństwo systemów informatycznych

dr Marek Miśkiewicz

October 23, 2020

Instytut Informatyki UMCS

Elementy kryptografii

- Kryptografia symetryczna i strumieniowa
- Uwierzytelnianie wiadomości
- Kryptografia asymetryczna - klucze publiczne i prywatne
- Podpisy cyfrowe

Elementy kryptografii

Kryptografia symetryczna

- Podstawowa metoda dla zapewnienia poufności transmitowanych danych.
- Oparta na pojedynczym kluczu szyfrującym.
- Dla zapewnienia bezpieczeństwa wymaga się:
  - silnego algorytmu
  - nadawca i odbiorca muszą posiadać (współdzielić) ten sam klucz (trzymany w sekrecie)

Kryptografia symetryczna

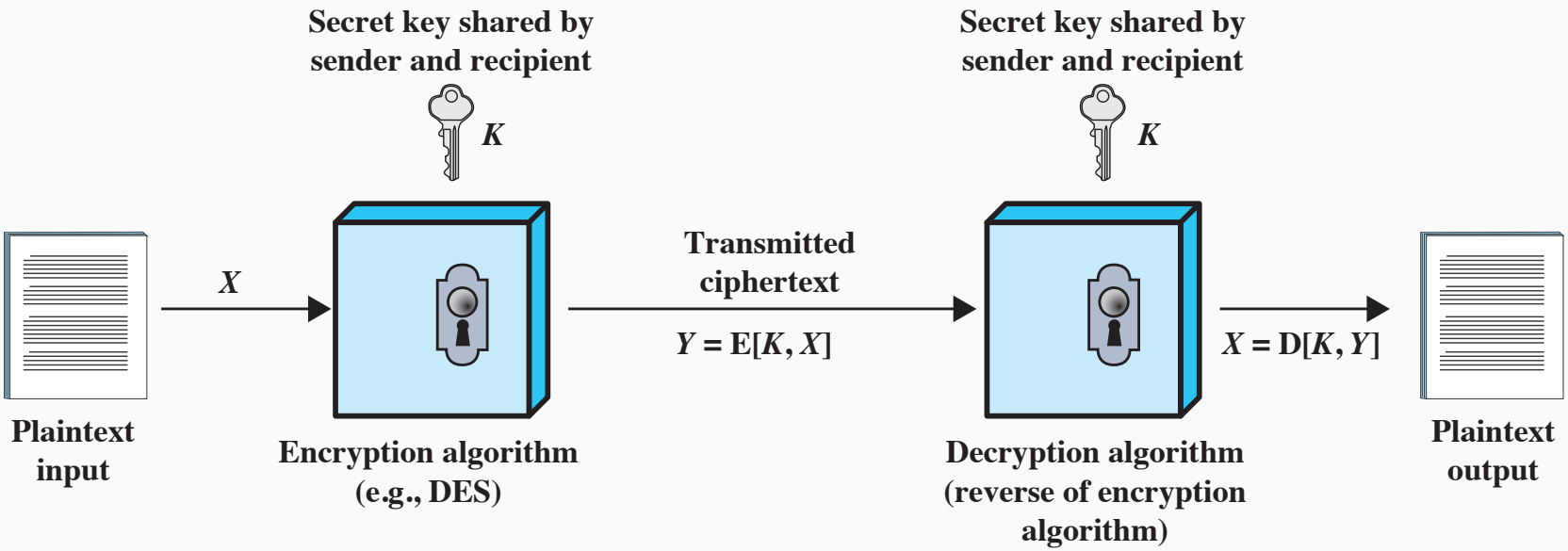


Figure 2.1 Simplified Model of Symmetric Encryption

Ataki kryptoanalityczne

- Bazują na:
  - ”naturze” algorytmu
  - wiedzy na temat charakterystyki tekstu jawnego
  - próbkach tekstu jawnego i szyfrogramu
- Wykorzystują charakterystyczne cechy algorytmu do odkrycia właściwości użytego tekstu jawnego lub klucza. Celem jest najczęściej **ujawnienie klucza**, co z kolei oznacza, że wszystkie szyfrogramy powiązane z tym kluczem zostają ”skompromitowane”.

Kryptografia symetryczna - ataki

Ataki typu ”brute-force”

- W tym przypadku przegląda się całą przestrzeń kluczy, deszyfrując szyfrogram w poszukiwaniu ”sensownego” tekstu jawnego. W rzeczywistości zazwyczaj wystarcza przejrzenie połowy wszystkich kluczy.

Porównanie DES, 3DES i AES

DES - Data Encryption Standard

3DES - Triple DES

AES - Advanced Encryption Standard

	DES	3DES	AES
Plaintext block size (bits)	64	64	128
Cipher text block size (bits)	64	64	128
Key size (bits)	56	112, 168	128, 192, 256

Kryptografia symetryczna

DES

- Do niedawna najczęściej stosowany
- Określany jak DEA - Data Encryption Standard
- Używa 65 bitowych bloków tekstu jawnego i klucza 56 bitowego produkując 64 bitowy szyfrogram

Podatności:

- Najlepiej zbadany algorytm (analitycznie)
- Przy współczesnej szybkości obliczeniowej długość klucza jest ”żałośnie” niewystarczająca

Kryptografia symetryczna

Średni czas potrzebny na znalezienie klucza:

Klucz (bity)	Algorytm	Liczba kluczy	10^9 dec/s	10^{13} dec/s
56	DES	$2^{56} \approx 7.2 \cdot 10^{16}$	$2^{55}\text{ns} = 1.125\text{y}$	1 h
128	AES	$2^{128} \approx 3.4 \cdot 10^{38}$	$2^{127}\text{ns} = 5 \cdot 10^{21} y$	$5.3 \cdot 10^{17}$ y
168	3 DES	$2^{168} \approx 3.7 \cdot 10^{50}$	$2^{167}\text{ns} = 5.8 \cdot 10^{33} y$	$5.8 \cdot 10^{29} y$
192	AES	$2^{192} \approx 6.3 \cdot 10^{57}$	$2^{191}\text{ns} = 9.8 \cdot 10^{40} y$	$9.8 \cdot 10^{36} y$
256	3 AES	$2^{256} \approx 1.2 \cdot 10^{77}$	$2^{255}\text{ns} = 5.8 \cdot 10^{60} y$	$1.8 \cdot 10^{56} y$

3DES - Triple DES

- Powiela trzykrotnie algorytm DES używając dwóch lub trzech unikalnych kluczy
- ANSI standard X9.17 dla operacji finansowych (1985)
- Zalety:
  - klucz 168 bitowy znacznie utrudnia ataki brute-force
  - u podstawy zwykły algorytm DES
- Wady:
  - powolna implementacja sprzętowa
  - nadal tylko 64 bitowe bloki danych

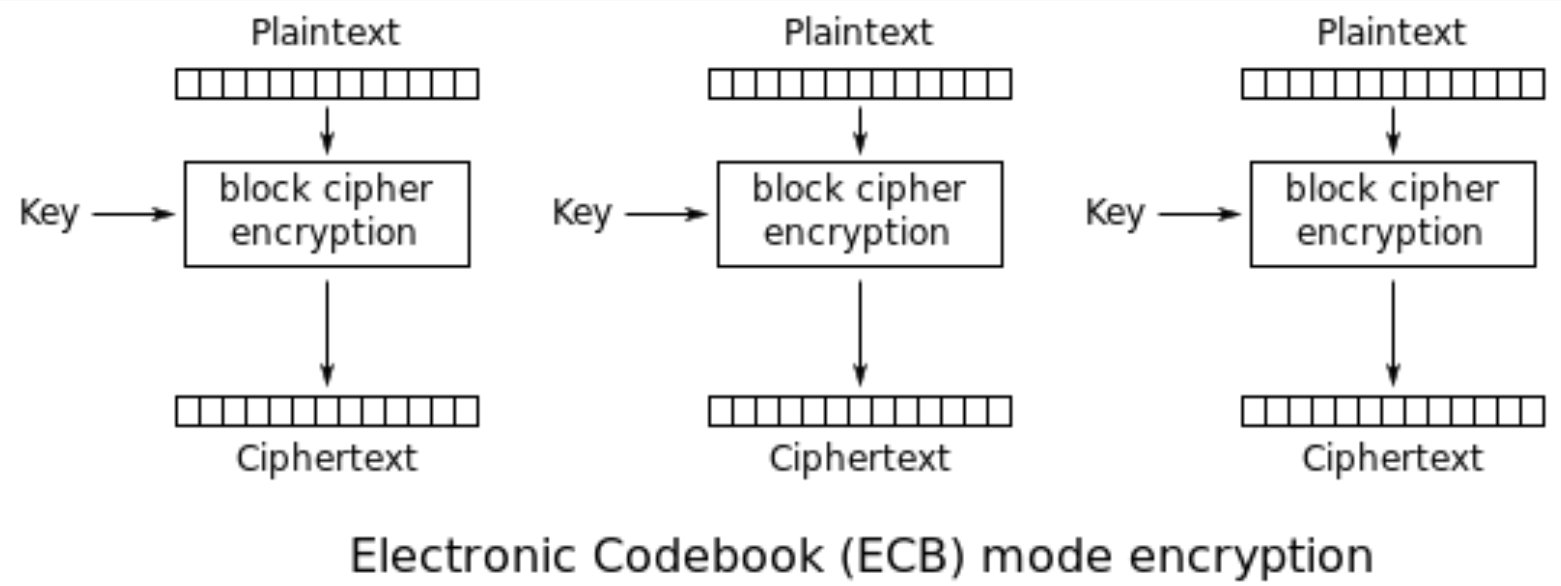
AES - Advanced Encryption Standard

- Konieczność zastąpienia 3DES'a , który w perspektywie długoterminowej nie nadawał się do użycia
- Konkurs NIST:
  - Bezpieczeństwo na poziomie nie niższym niż 3DES
  - Duża wydajność (szybkość algorytmu)
  - symetryczny szyfr blokowy
  - bloki 128 bitowe i klucz o rozmiarach 128, 192, 256 bitów
- Rijandael (listopad 2001) wybrany jako AES

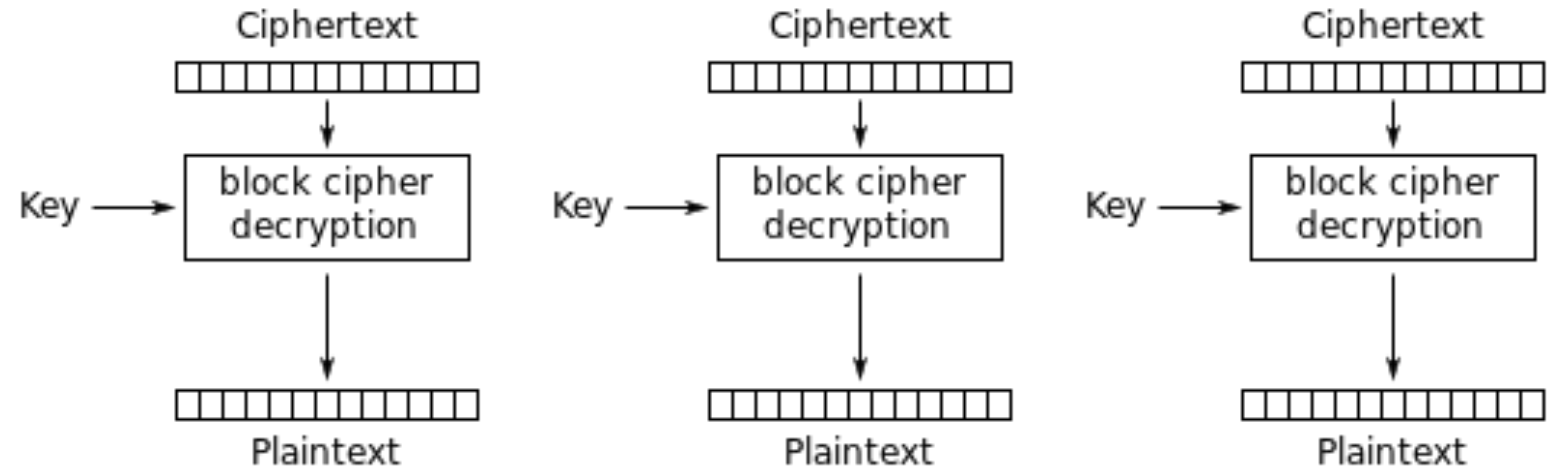
Kwestje bezpieczeństwa

- Zazwyczaj szyfrowanie symetryczne stosuje dię do bloku danych o rozmiarze 64 lub 128 bitowe. Oznacza to konieczność dzielenia danych wejściowych na bloki.
- **tryb ECB** (Electronic Code Book) - każdy blok jest szyfrowany tym samym kluczem - podejście najprostsze ale najbardziej niebezpieczne - mamy wiele szyfrogramów za szyfrowanych tym samym kluczem.
- **Tryb CBC** (Cipher block chaining) - kolejne bloki tekstu jawnego przed szyfrowaniem są ”xorowane” z zaszyfrowanymi blokami poprzedzającymi

Tryb ECB

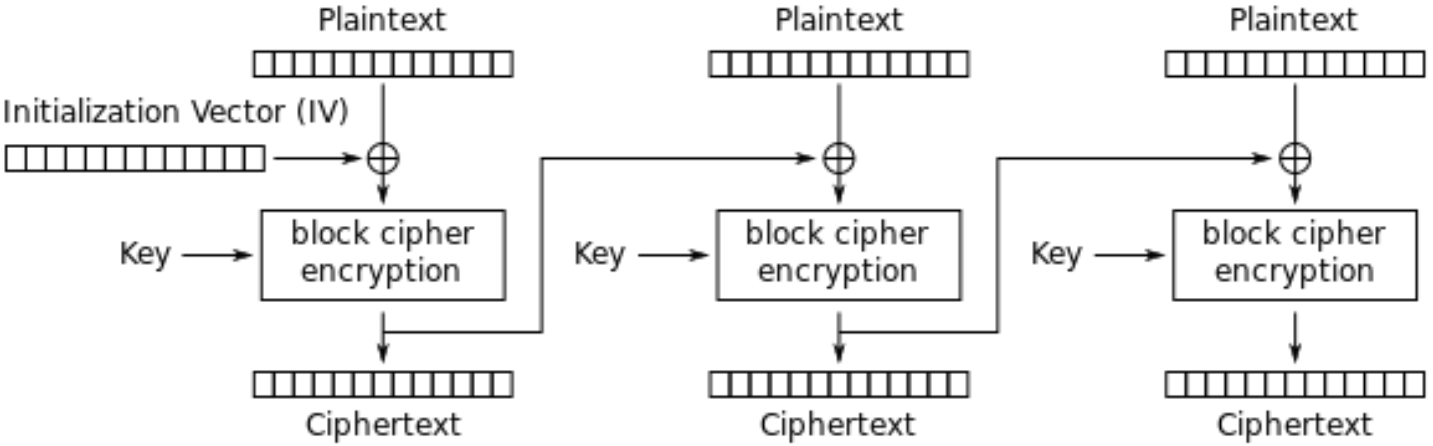


Electronic Codebook (ECB) mode encryption

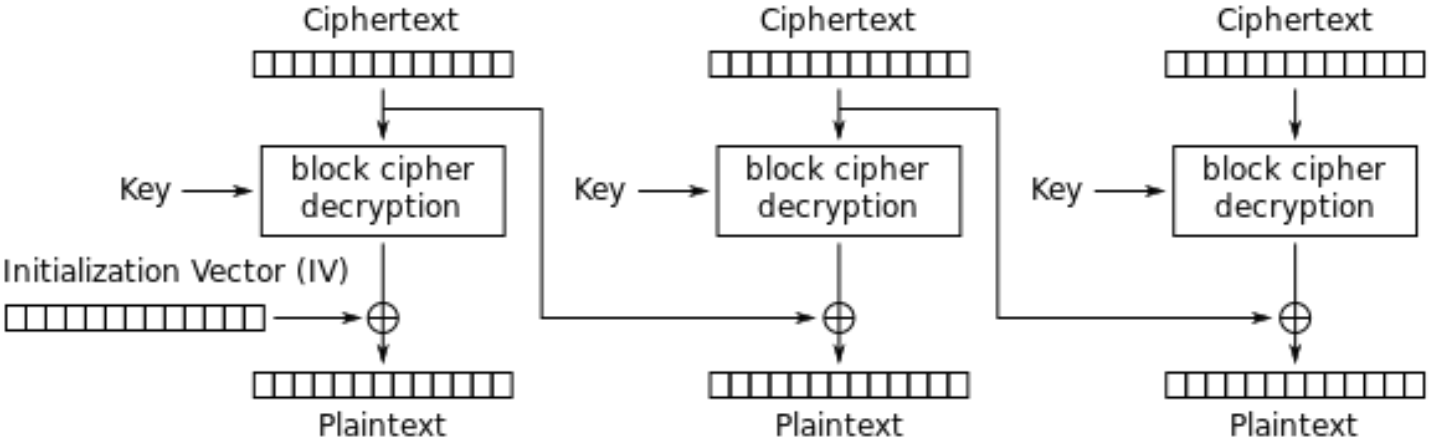


Electronic Codebook (ECB) mode decryption

Tryb cbc

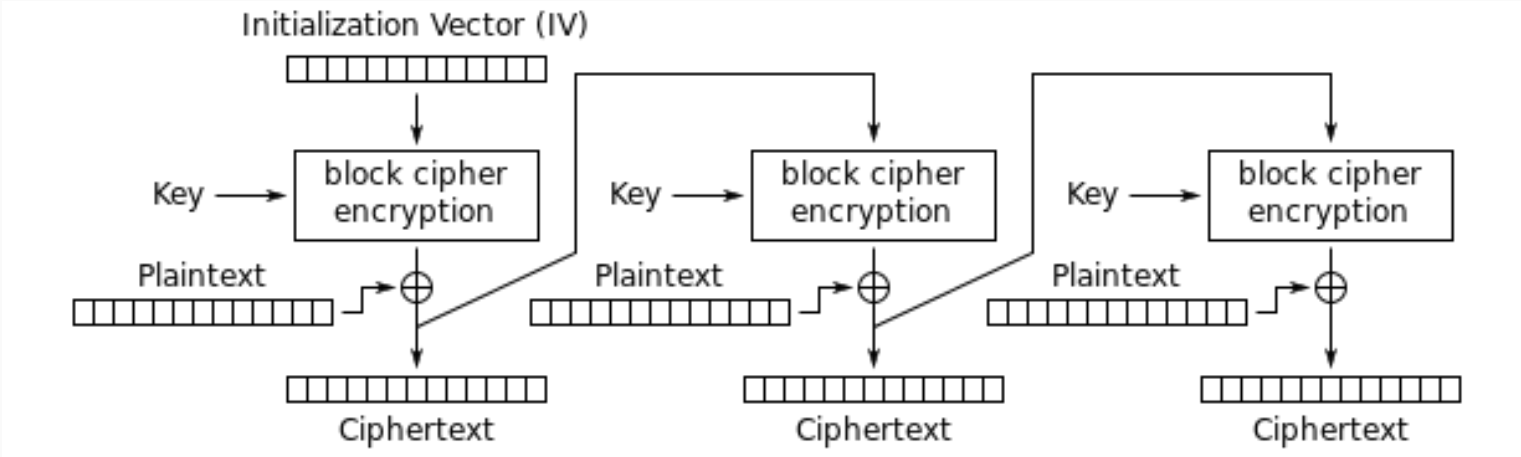


Cipher Block Chaining (CBC) mode encryption

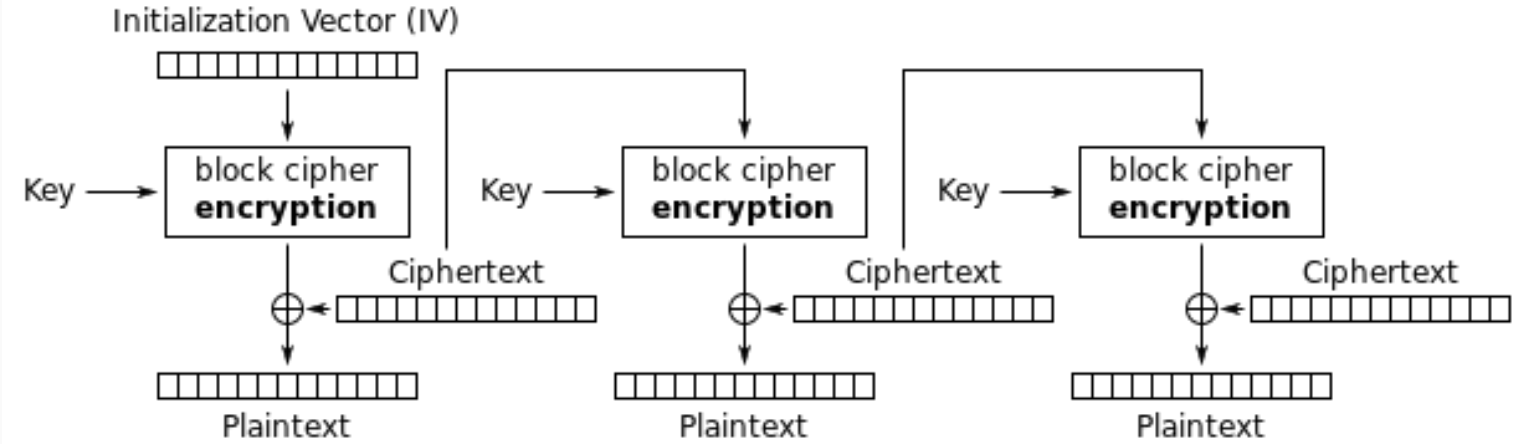


Cipher Block Chaining (CBC) mode decryption

Tryb CFB

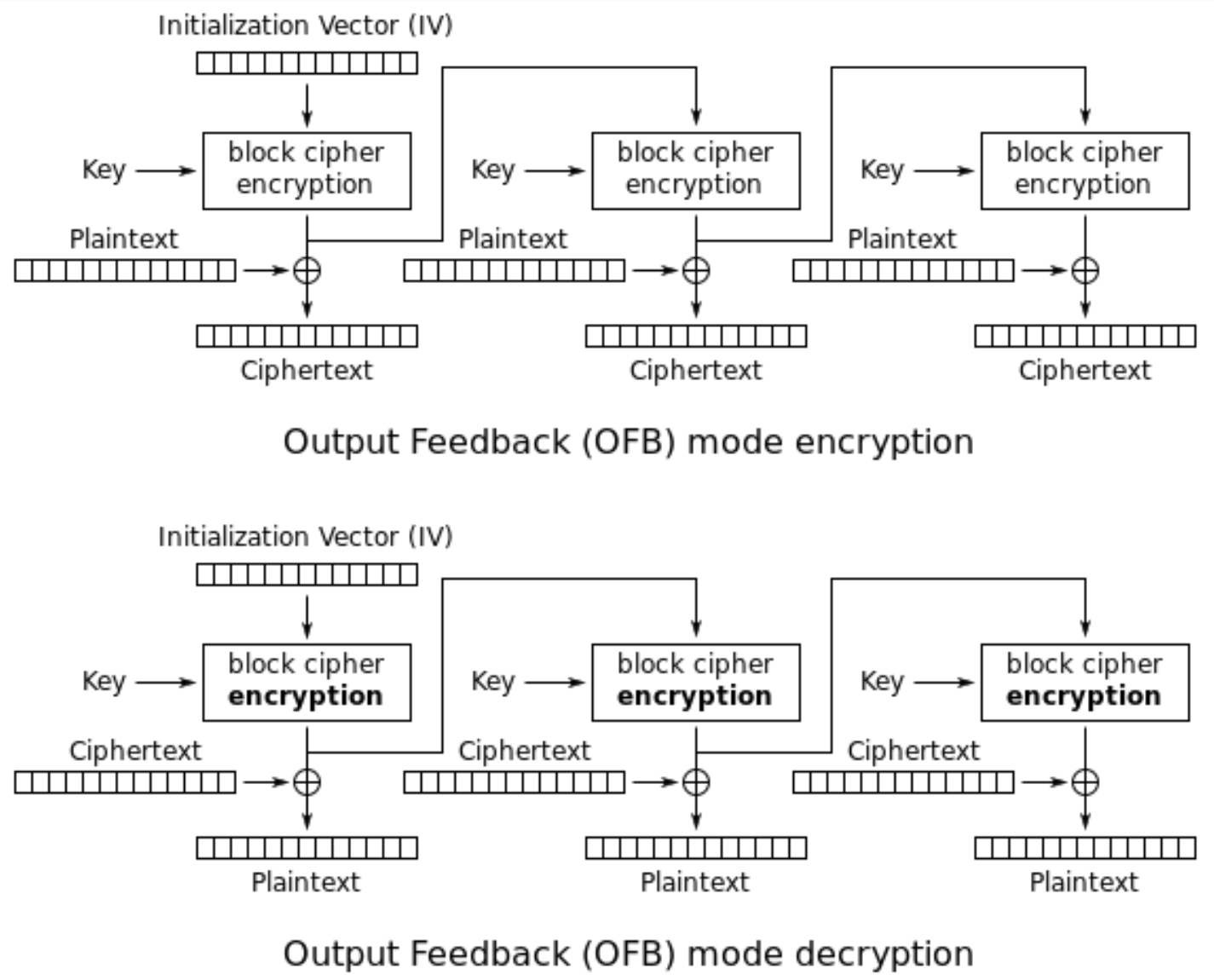


Cipher Feedback (CFB) mode encryption

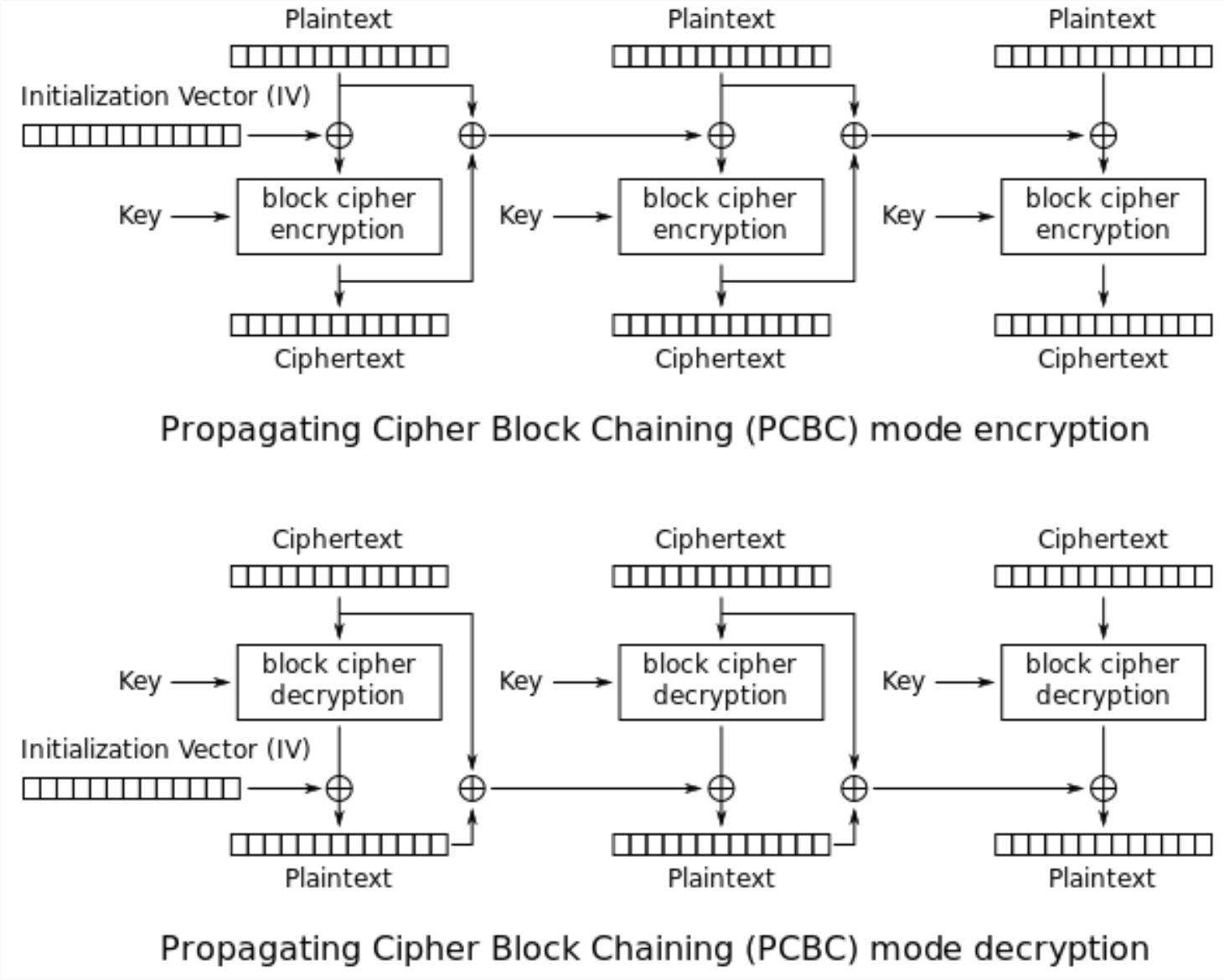


Cipher Feedback (CFB) mode decryption

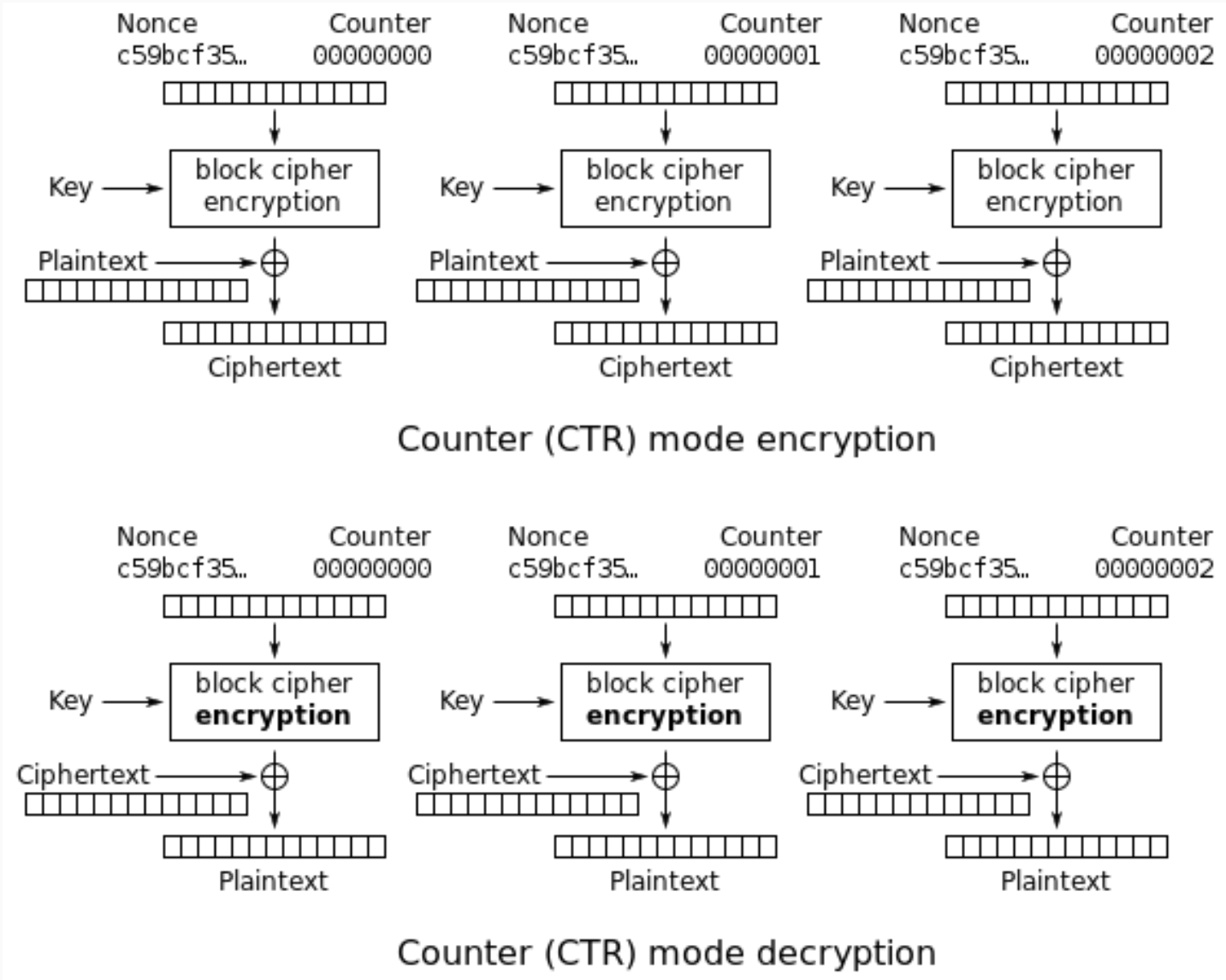
Tryb OFB


Initialization Vector (IV)
Key
block cipher encryption
Plaintext
Ciphertext
Output Feedback (OFB) mode encryption
Initialization Vector (IV)
Key
block cipher encryption
Ciphertext
Plaintext
Output Feedback (OFB) mode decryption

Tryb PCBC


Plaintext
Plaintext
Plaintext
Initialization Vector (IV)
Key
block cipher encryption
Key
block cipher encryption
Key
block cipher encryption
Ciphertext
Ciphertext
Ciphertext
Propagating Cipher Block Chaining (PCBC) mode encryption
Ciphertext
Ciphertext
Ciphertext
Key
block cipher decryption
Key
block cipher decryption
Key
block cipher decryption
Initialization Vector (IV)
Plaintext
Plaintext
Plaintext
Propagating Cipher Block Chaining (PCBC) mode decryption

Tryb CTR


Nonce
c59bcf35...
Counter
00000000
00000001
00000002
Key
block cipher encryption
Plaintext
Ciphertext
Counter (CTR) mode encryption
block cipher encryption
Counter (CTR) mode decryption

Szyfry blokowe a szyfry strumieniowe

Szyfry blokowe

- dane wejściowe przetwarzane są po jednym bloku elementów naraz
- tworzony jest blok wyjściowy dla każdego bloku wejściowego
- klucz używany jest wielokrotnie
- duża powszechność

Szyfry strumieniowe

- szyfrują dane wejściowe w sposób ciągły
- bajt (bit) wej. $\longrightarrow$ bajt (bit) wyj.
- duża szybkość działania $\leftrightarrow$ bardzo proste algorytmy
- maksymalna entropia szyfrogramu dla ”losowego klucza”

W domu

Trzy przykłady szyfrów blokowych.

Trzy przykłady szyfrów strumieniowych

Uwierzytelnianie wiadomości

- Ochrona przed atakami aktywnymi
- Wiadomość zweryfikowana jest ”autentyczna”
  - nie zmieniono treści - **integralność**
  - potwierdzone źródło - **niezaprzeczalność**
  - czas i właściwa kolejność
- Można wykorzystać kryptografię symetryczną (przy założeniu, że tylko nadawca i odbiorca współdzielą klucz)

Uwierzytelnianie wiadomości bez zachowania poufności

- Szyfrowanie wiadomości nie zapewnia bezpiecznej formy uwierzytelnienia
- Można połączyć uwierzytelnienie i poufność w jednym algorytmie szyfrując wiadomość oraz podpis uwierzytelniający
- Najczęściej, podpis wiadomości zapominany jest poprzez oddzielną funkcję

Uwierzytelnianie wiadomości bez zachowania poufności

- Sytuacje, gdzie uwierzytelnienie bez szyfrowania może być preferowane:
  - komunikaty rozsyłane tekstem jawnym do wielu odbiorców (sieć)
  - ”heavy load” - brak czasu na deszyfrowanie
  - podpisywanie programów komputerowych

Kryptografia symetryczna

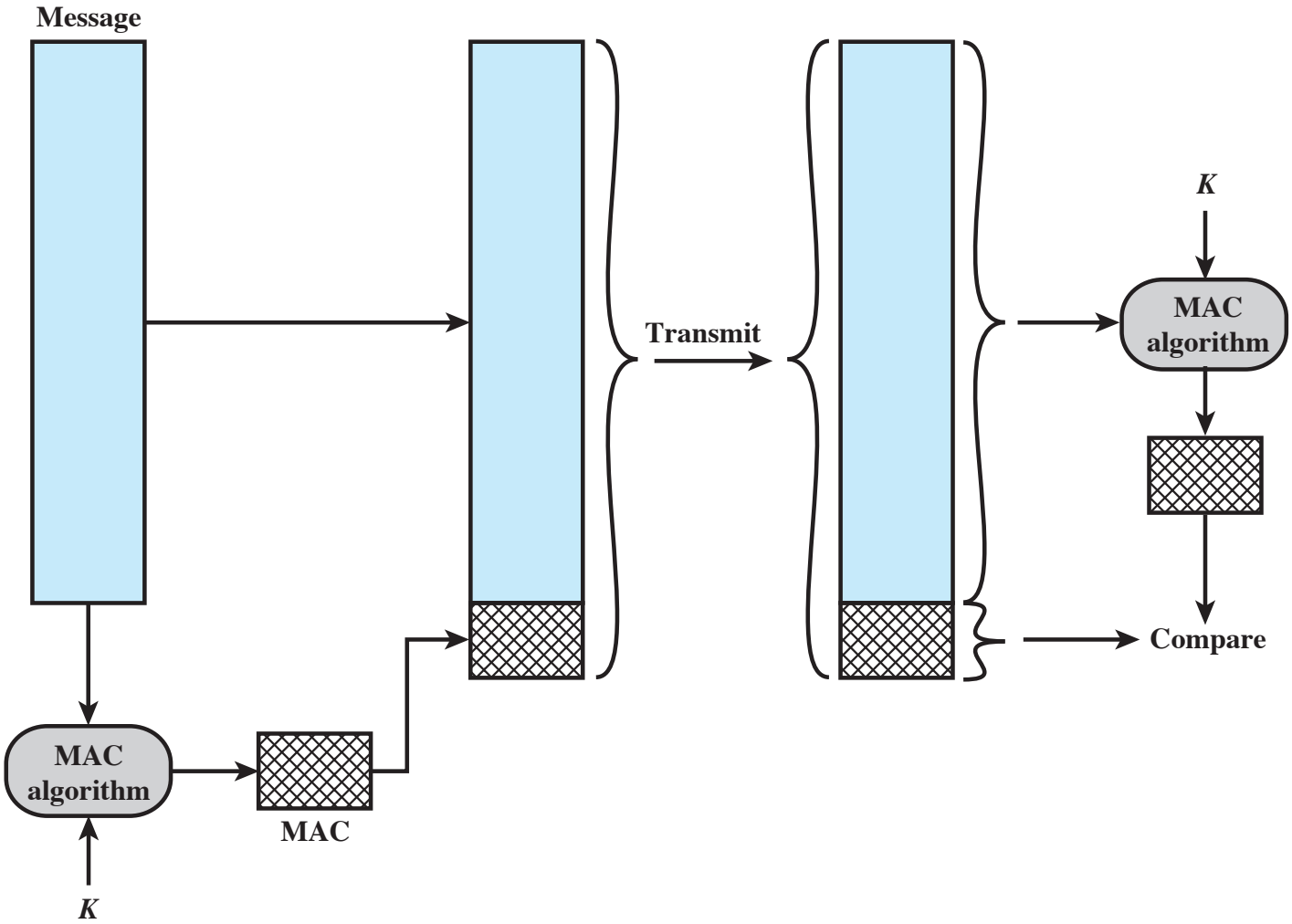
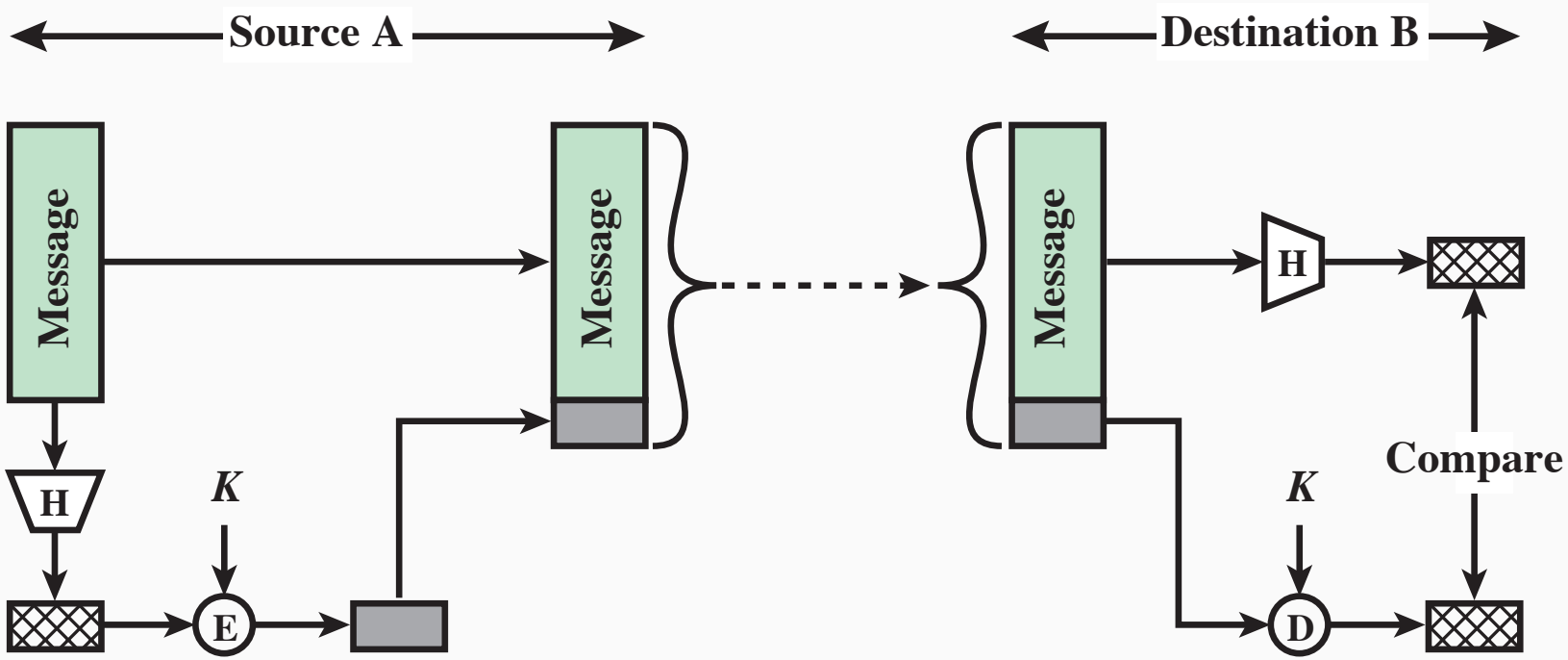


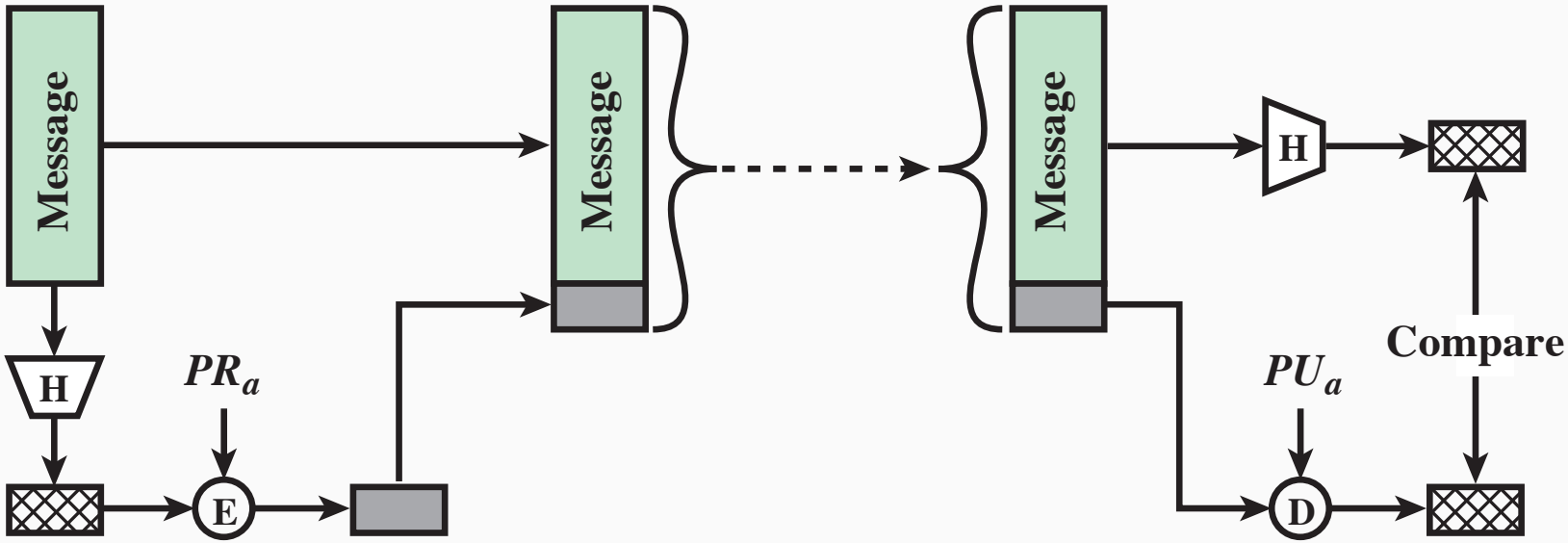
Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).

Kryptografia symetryczna



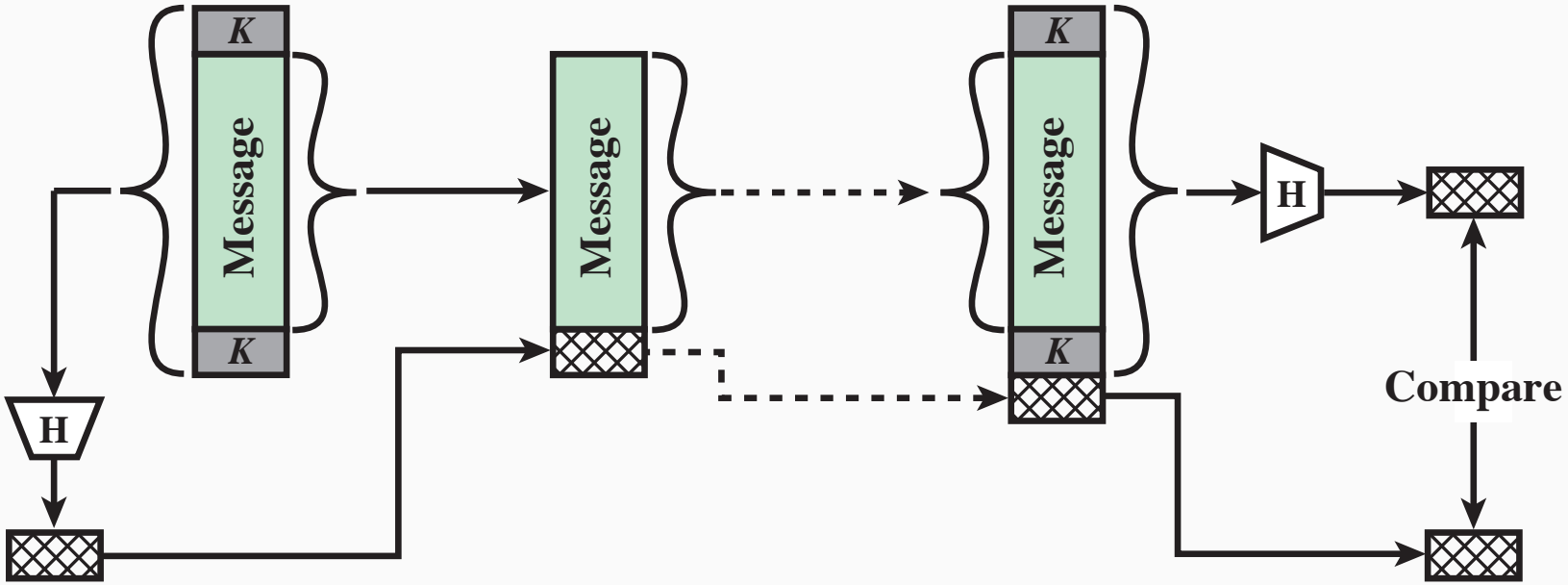
(a) Using symmetric encryption

Kryptografia symetryczna



(b) Using public-key encryption

Kryptografia symetryczna



(c) Using secret value

Jednokierunkowe funkcje skrótu

- MD5 - Message-Digest algorithm 5: ”dowolny ciąg wejściowy” $\longrightarrow$ kod 128 bitowy
  ”marek” $\longrightarrow$ e061c9aea5026301e7b3ff09e9aca2cf
- SHA - Secure Hash Algorithm

Algorytm		Rozmiar skrótu	Kolizje
	SHA-0	160	Tak
	SHA-1	160	Tak (2^{51})
SHA-2	SHA-256/224	256/224	Nie
SHA-2	SHA-512/384	512/384	Nie

Funkcje skrótu $H(x)$

Właściwości:

- działa an bloku danych dowolnej długości
- produkuje wynik określonej stałej długości
- $H(x)$ musi być ”łatwa” do obliczenia dla danego x
- jednokierunkowa, ”pre-image resistant”
- odporna na kolizje ($x \neq y \quad$ i $\quad H(x) = h(y)$)

Funkcje skrótu - kwestje bezpieczeństwa

Metody kryptoanalityczne - wykorzystanie słabości algorytmu

Metody ”Brute-force” - siła funkcji skrótu zależy od długości skrótu, który funkcja generuje

Funkcje jednokierunkowe (niekonieczne haszujące):

- **PBKDF** - Password Based Key Derivation Function
- **bcrypt** - ”work factor”

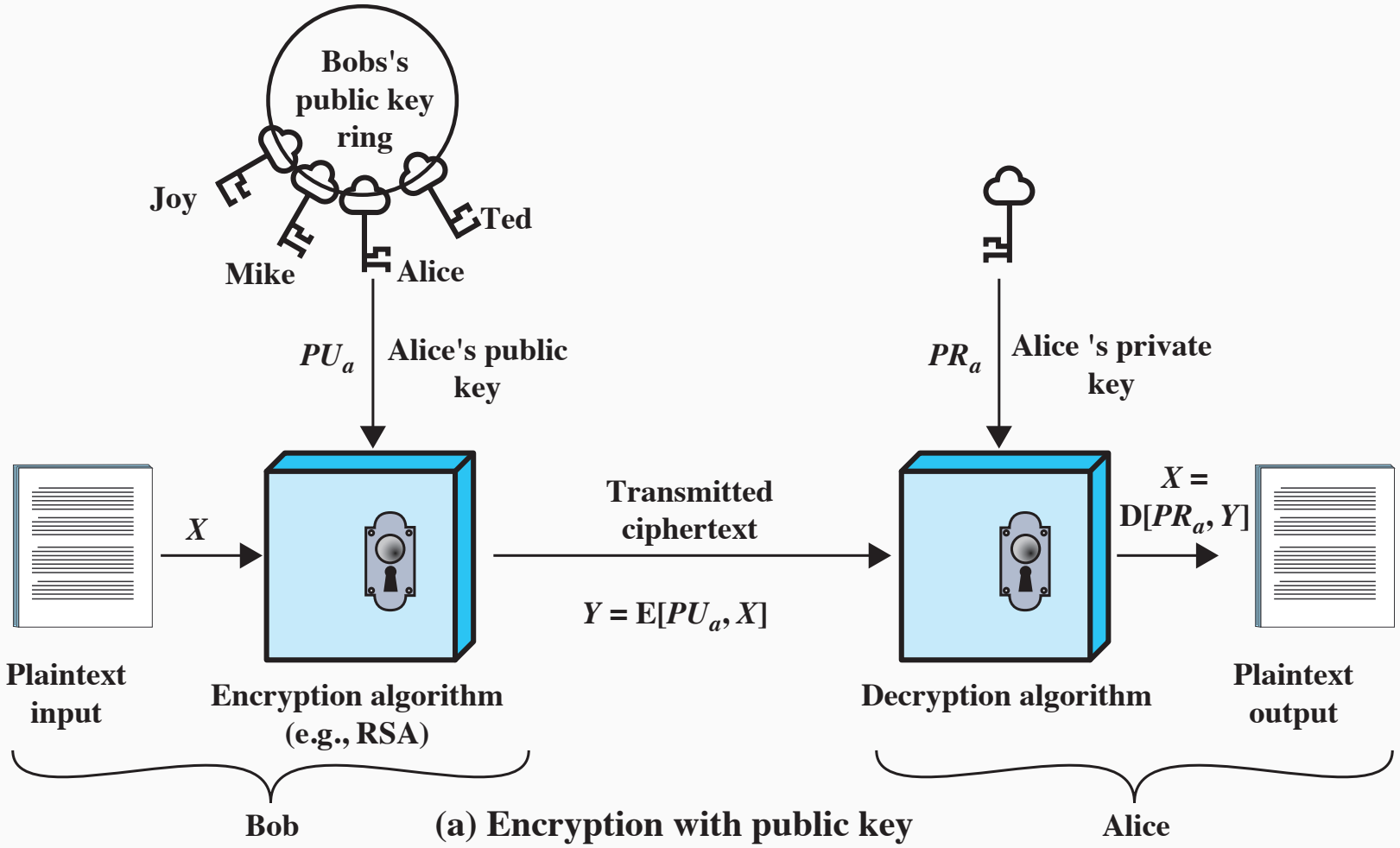
Funkcje skrótu

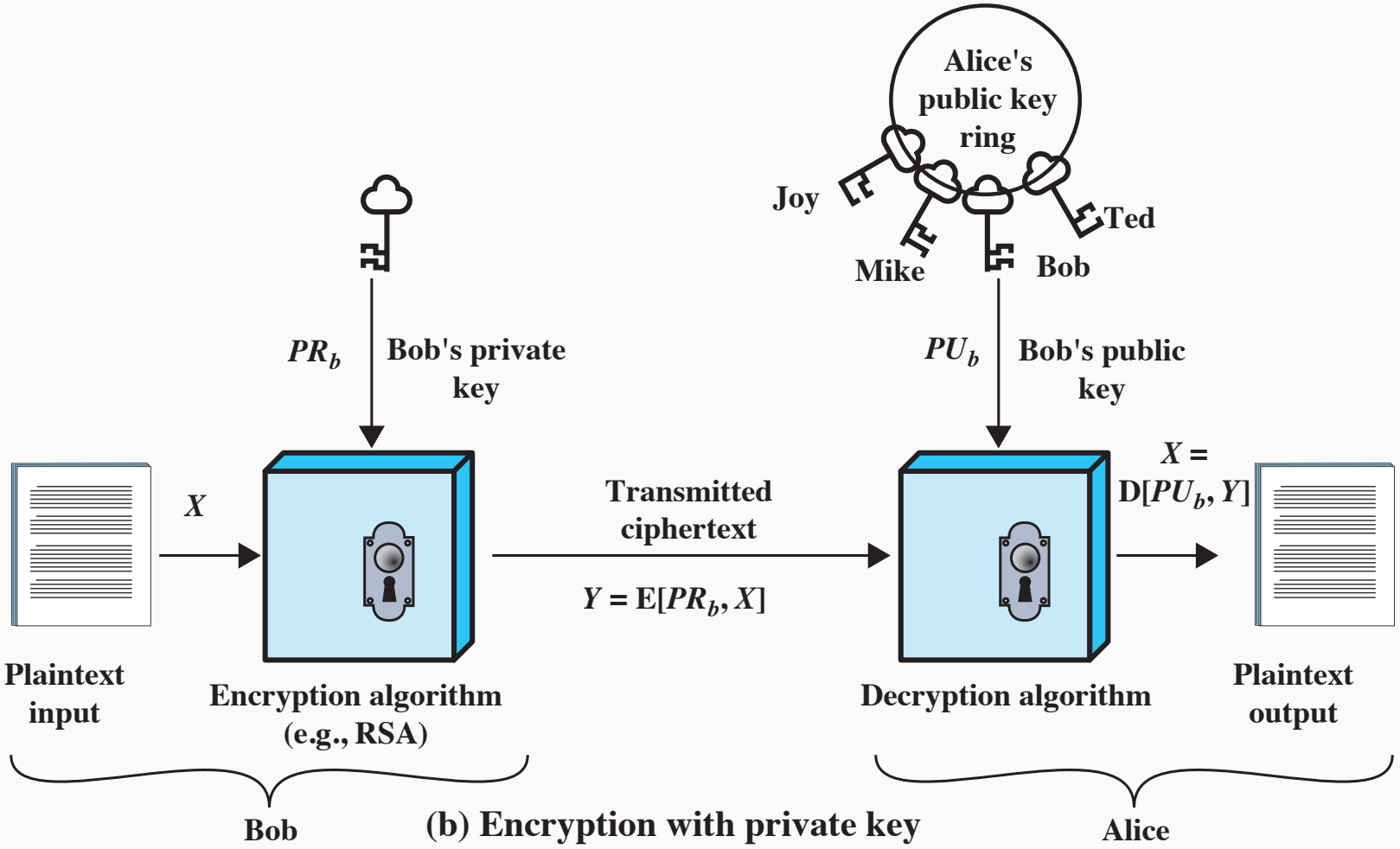
Inne aplikacje:

- sposób zapisywania haseł w systemie
- IDS - Intrusion Detection - zapisywanie w ”bezpieczny sposób” skrótów plików

Kryptografia asymetryczna

- Koncepcja zaproponowana przez Diffie'go i Hellmana w 1976 r.
- Bazuje na algebrze dyskretnej
- Asymetryczność:
  - dwa "sprzężone klucze":
  - **klucz prywatny** - trzymany w sekrecie
  - **klucz publiczny** - dostępny publicznie
- Rozwiązuje problem dystrybucji klucza


Bobs's public key ring
Joy
Ted
Mike
Alice
PU_a
Alice's public key
PR_a
Alice 's private key
X
Transmitted ciphertext
$Y = E[PU_a, X]$
$X = D[PR_a, Y]$
Plaintext input
Encryption algorithm (e.g., RSA)
Decryption algorithm
Plaintext output
Bob
(a) Encryption with public key
Alice



UWAGA

Szyfrowanie **kluczem prywatnym** ma tu szczególny sens!

Kryptografia asymetryczna

Systemy kryptograficzne bazujące na koncepcji klucza publicznego:

Algorytm	Podpis cyfrowy	Dystrybucja klucza sym.	Szyfrowanie kluczy
RSA	tak	tak	tak
Diffie-Hellman	nie	tak	nie
DSS	tak	nie	nie
Elliptic Curve	tak	tak	tak

Kryptografia asymetryczna

Wymagania:

- łatwość wyliczania pary kluczy
- wydajny system dystrybucji kluczy publicznych
- duża złożoność obliczeniowa dla próby ustalenia klucz prywatnego na podstawie publicznego
- łatwość w odszyfrowaniu wiadomości z wykorzystaniem klucza prywatnego
- ”silny” algorytm szyfrujący

Kryptografia asymetryczna - algorytmy

- RSA - Rivest, Shamir, Adleman
  - wynaleziony w 1977 r. i szeroko stosowany
  - bazuje na problemie faktoryzacji (dane to liczby z przedziału od 0 to $n - 1$ dla pewnego n)
  - udana faktoryzacja klucza 768 bitowego
  - akceptowane kucze (ze względu na bezpieczeństwo) 2048 i 4096 bitów
  - duże zagrożenie stanowi ”komputer kwantowy”

Kryptografia asymetryczna - algorytmy

- **Protokół wymiany klucza Diffie'go - Hellmana**
  - pozwala dwóm użytkownikom na bezpieczną wymianę klucza lub sekretu - jedyna funkcja algorytmu (możliwe rozszerzenia na większa liczbę użytkowników)
  - intruz w kanale komunikacyjnym na podstawie przechwyconych danych nie jest w stanie ustalić wartości klucza $\longrightarrow$ możliwy jest jednak atak typu "man-in-the-middle"

Algorytm wymiany klucza diffie'go-Hellmana

Alicja	
wie	nie wie
$p = 23$	$b = ?$
podstawa $g = 5$	
$a = 6$	
$A = 5^6 \bmod 23 = 8$	
$B = 5^b \bmod 23 = 19$	
$s = 19^6 \bmod 23 = 2$	
$s = 8^b \bmod 23 = 2$	
$s = 19^6 \bmod 23 = 8^b \bmod 23$	
$s = 2$	

Bob	
wie	nie wie
$p = 23$	$a = ?$
podstawa $g = 5$	
$b = 15$	
$B = 5^{15} \bmod 23 = 19$	
$A = 5^a \bmod 23 = 8$	
$s = 8^{15} \bmod 23 = 2$	
$s = 19^a \bmod 23 = 2$	
$s = 8^{15} \bmod 23 = 19^a \bmod 23$	
$s = 2$	

Ewa	
wie	nie wie
$p = 23$	$a = ?$
podstawa $g = 5$	$b = ?$
	$s = ?$
$A = 5^a \bmod 23 = 8$	
$B = 5^b \bmod 23 = 19$	
$s = 19^a \bmod 23$	
$s = 8^b \bmod 23$	
$s = 19^a \bmod 23 = 8^b \bmod 23$	

Ewa nie jest w stanie poznać wartości sekretu s mimo stałej obecności w kanale komunikacyjnym.

Kryptografia asymetryczna - algorytmy

- DSS - Digital Signature Standard
  - standard NIST dla podpisów cyfrowych
  - dopuszcza stosowanie algorytmów SHA-1 i SHA-2
- ECC - Elliptic Curve Cryptography
  - oparte na złożoności obliczeniowej dyskretnych logarytmów na krzywych eliptycznych
  - ECC oferuje bezpieczeństwo porównywalne do RSA przy znacznie krótszych kluczach
  - klucz RSA o długości 1024 bitów jest równoważny bezpieczeństwu klucza ECC o długości 160 bitów

Podpisy cyfrowe

NIST FIPS PUB 186-4 definiuje podpis cyfrowy jako:

”Wynik kryptograficznej transformacji danych, który odpowiednio zaimplementowany zapewnia mechanizm weryfikacja uwierzytelnienia pochodzenia, integralności danych i niezaprzeczalności podpisu.

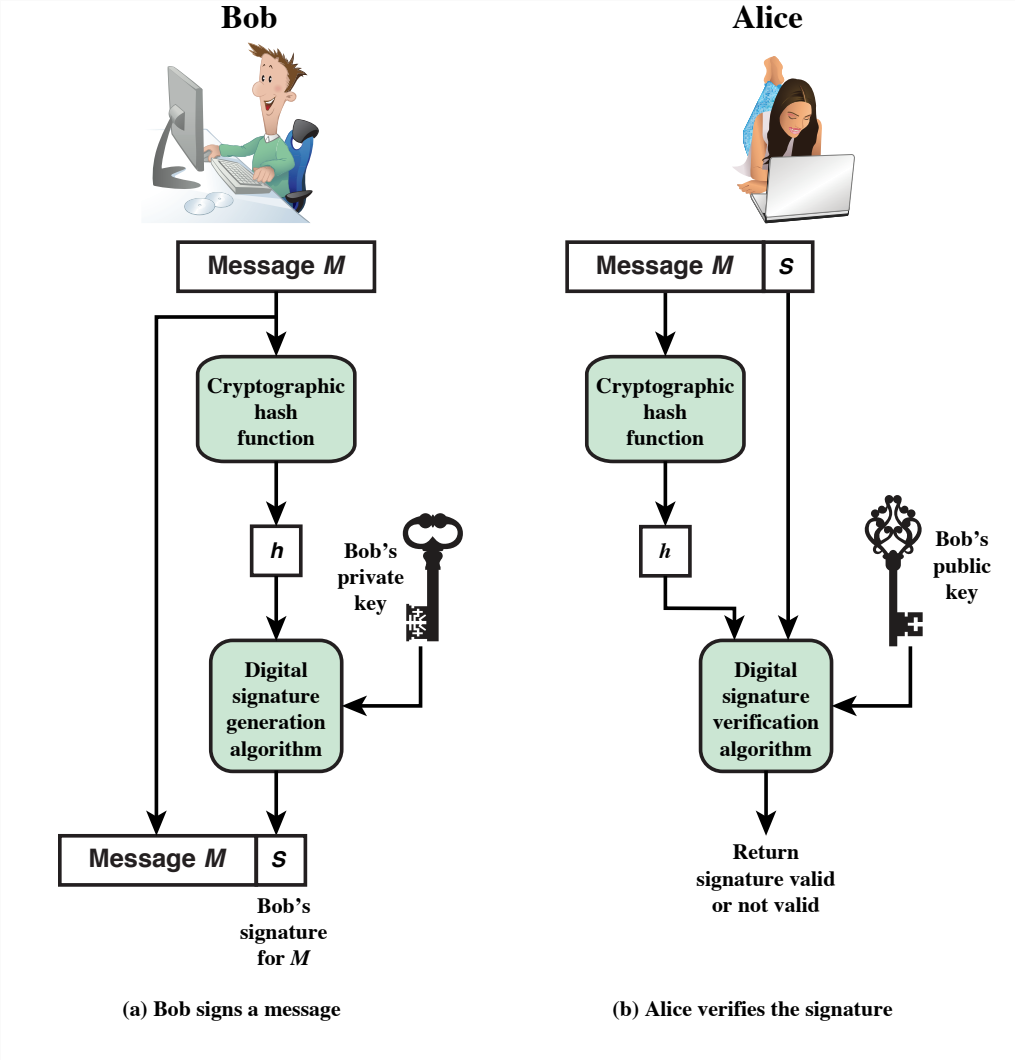
Podpis cyfrowy jest zależnym od danych wzorcem bitowym, generowanym przez algorytm jako funkcja pliku, wiadomości lub innej formy bloku danych.

Podpisy cyfrowe

FIPS 186-4 określa użycie jednego z trzech algorytmów podpisu cyfrowego:

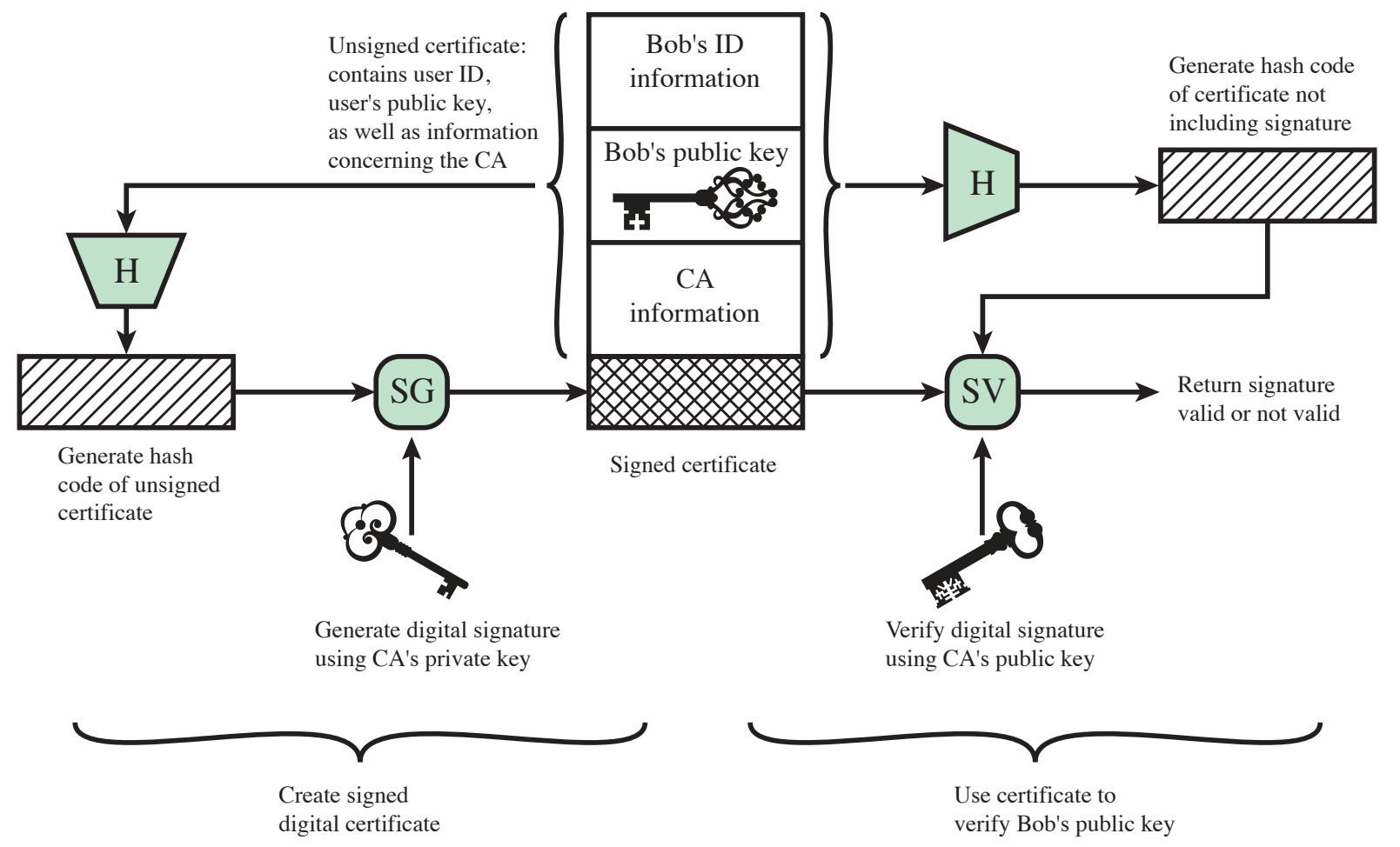
- DSA - Digital Signature Algorithm
- RSA Digital Signature Algorithm
- ECDSA - Elliptic Curve Digital Signature Algorithm

Idea podpisu cyfrowego



Uproszczone przedstawienie podstawowych elementów procesu skłdania podpisu cyfrowego

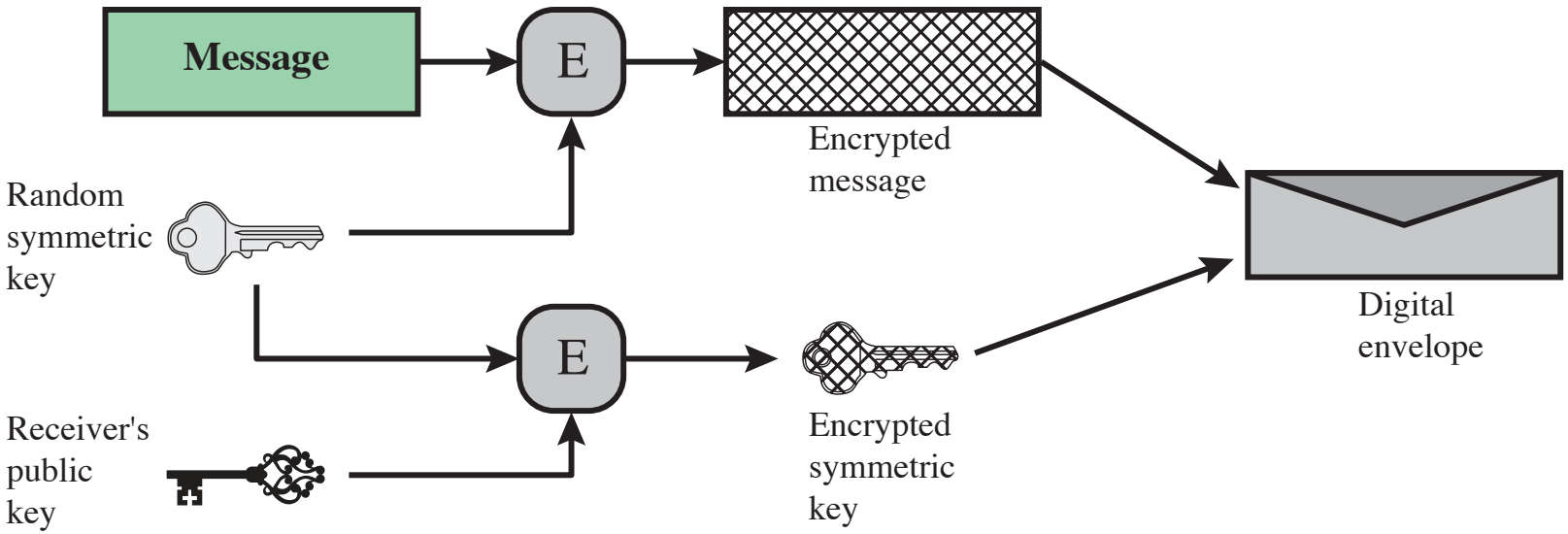
Poświadczenie certyfikatem



Koperta cyfrowa - szyfrowanie dużej ilości danych

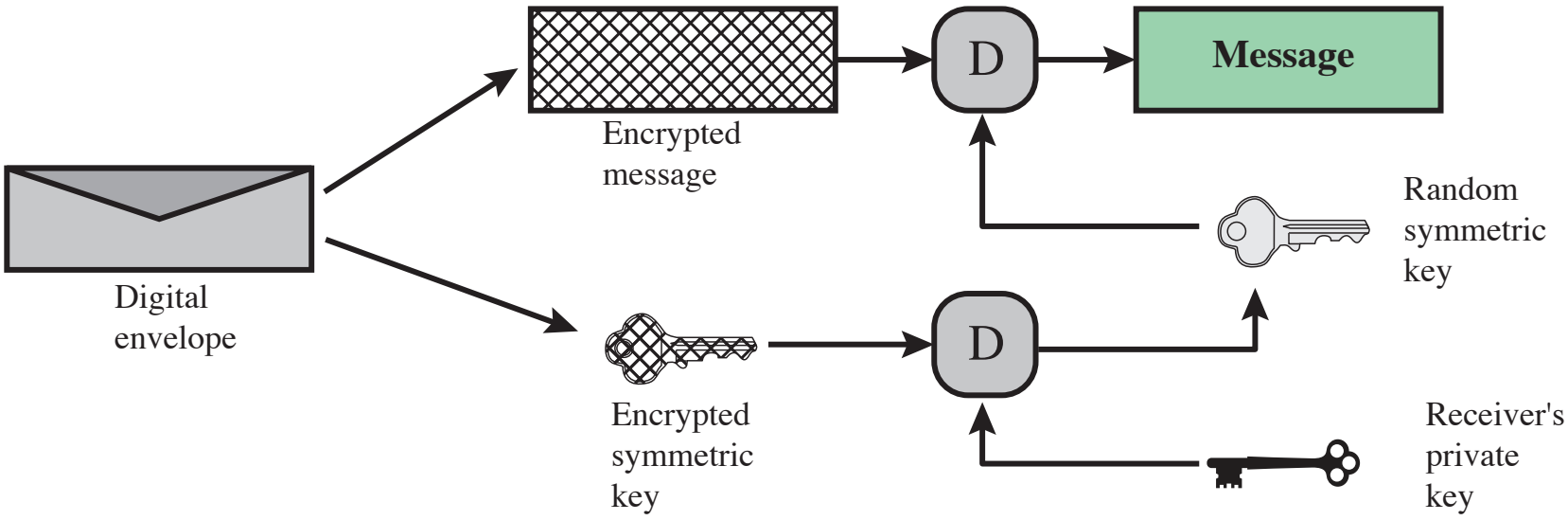
UWAGA

Kryptografia symetryczna posiada limit danych wejściowych dla szyfrowania!



(a) Creation of a digital envelope

Koperta cyfrowa - szyfrowanie dużej ilości danych



(b) Opening a digital envelope

W domu

GnuPG i PGP

Public Key Infrastructure

Bezpieczeństwo systemów informatycznych

dr Marek Miśkiewicz

November 15, 2020

Instytut Informatyki UMCS

MIME i S/MIME

MIME

MIME (Multipurpose Internet Mail Extension) jest rozszerzeniem starego standardu RFC 822 (Standard for The Format ARPA Internet Text Messages, 1982) zawierającego specyfikację formatu poczty internetowej. RFC 822 definiuje prosty nagłówek z polami `To`, `From`, `Subject` oraz innymi polami, które mogą być używane do kierowania wiadomości e-mail przez internet.

MIME udostępnia wiele nowych pól nagłówków, które definiują informacje o treści wiadomości, w tym dotyczące formatu treści i kodowania, co ma ułatwić przesyłanie.

S/MIME

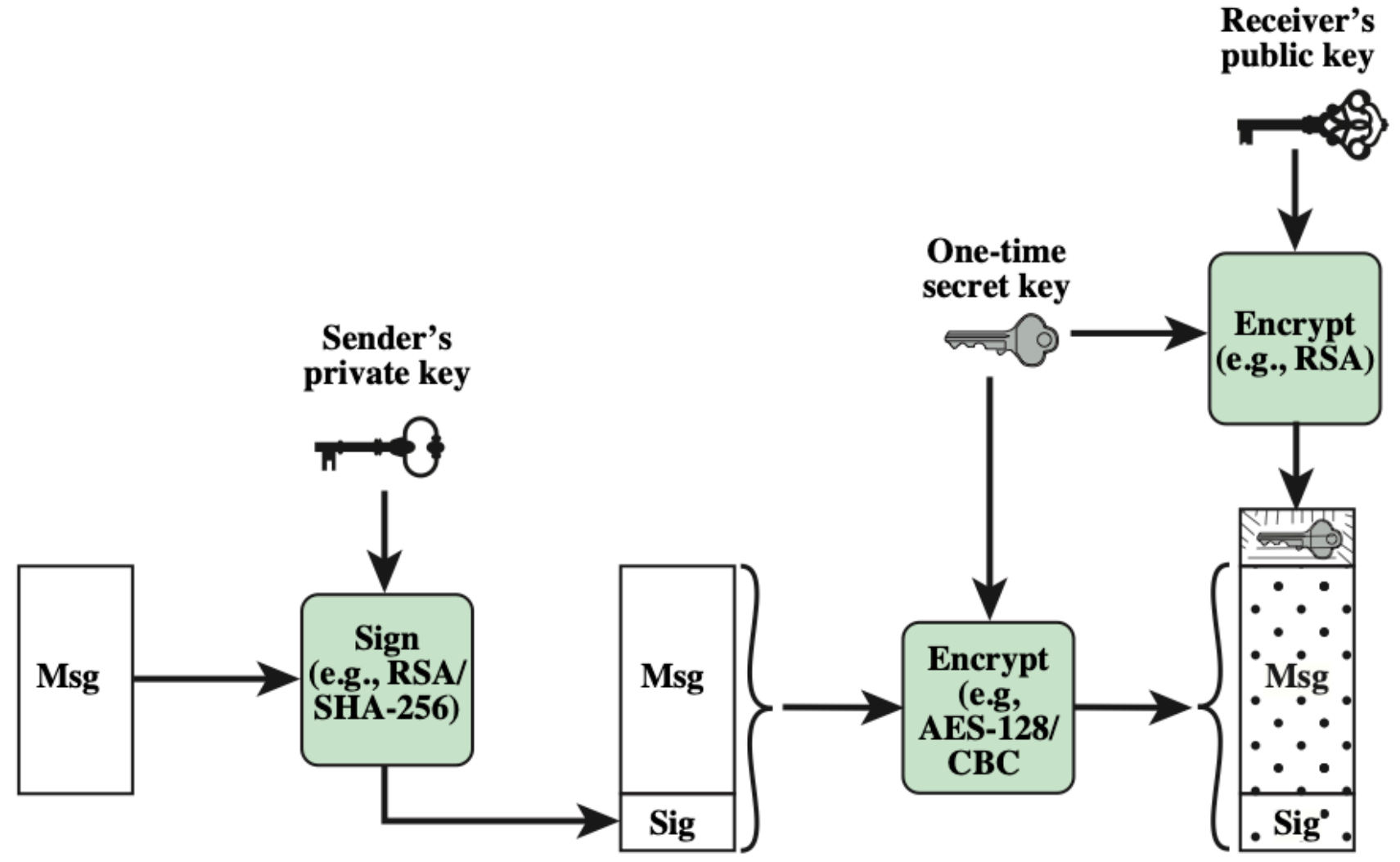
S/MIME (Secure/Multipurpose Internet Mail Extension) zestaw dodatkowych typów zawartości MIME. Nowe funkcje:

- Enveloped data - encrypted content and associated keys
- Signed data - encoded message + signed digest
- Clear-signed data - cleartext message + encoded signed digest
- Signed and enveloped data - nesting of signed and encrypted entities

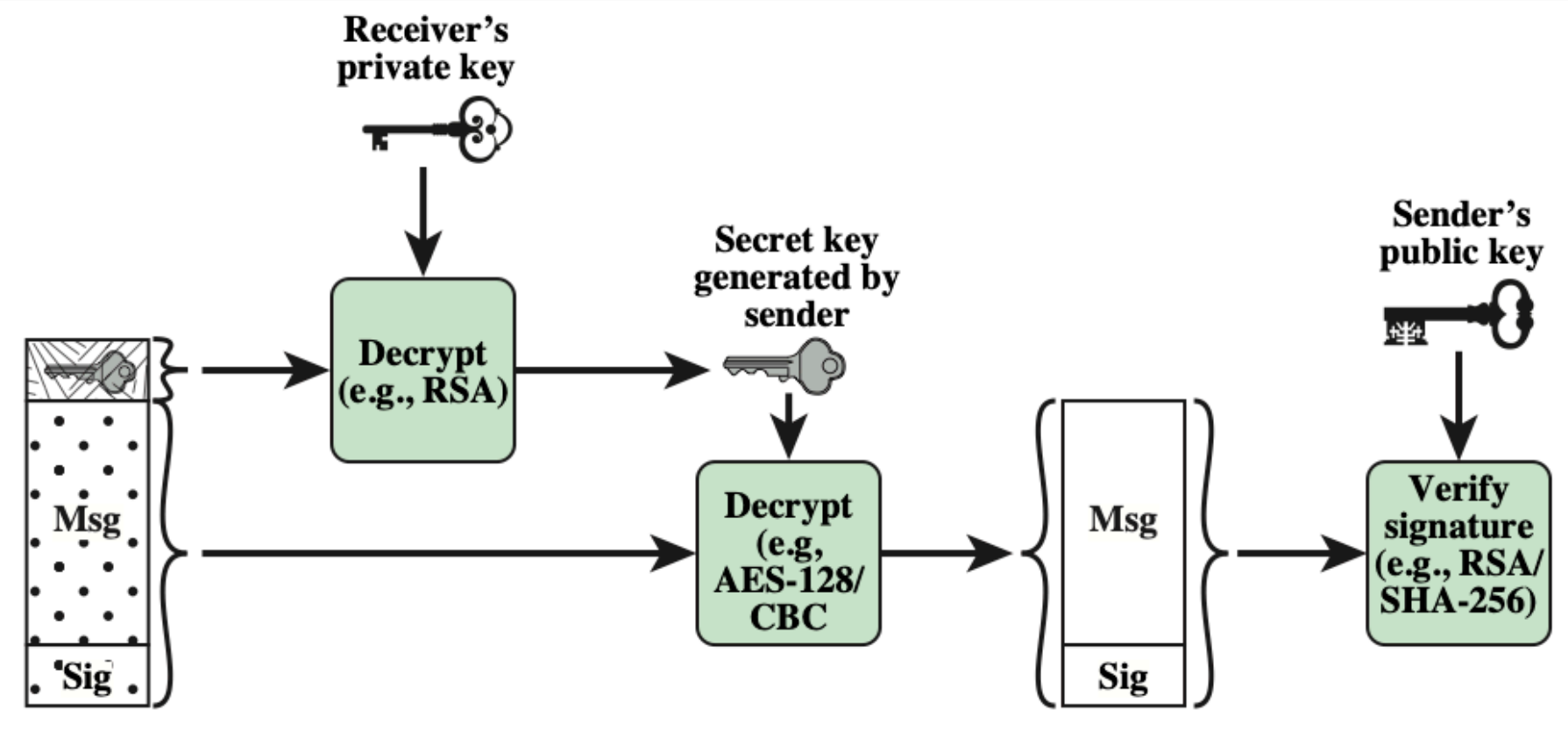
Typy zwartości S/MIME:

Typ	Podtyp	Parametr S/MIME	Opis
Multipart	Signed		Komunikat clear-signed w dwóch częściach: jedna to komunikat, a druga podpis
Application	pkcs7-mime	signedData	Podpisana encja S/MIME
	pkcs7-mime	envelopedData	Szyfrowana encja S/MIME
	pkcs7-mime	zdegenerowany obiekt singleData	Encja zawierająca wyłącznie certyfikaty klucza publicznego
	pkcs7-mime	CompressedData	Skompresowana encja S/MIME
	pkcs7-signature	signedData	Typ zawartości podczęści z podpisem wiadomości multipart/signed

S/MIME



Szyfrowanie i podpisywanie wiadomości.



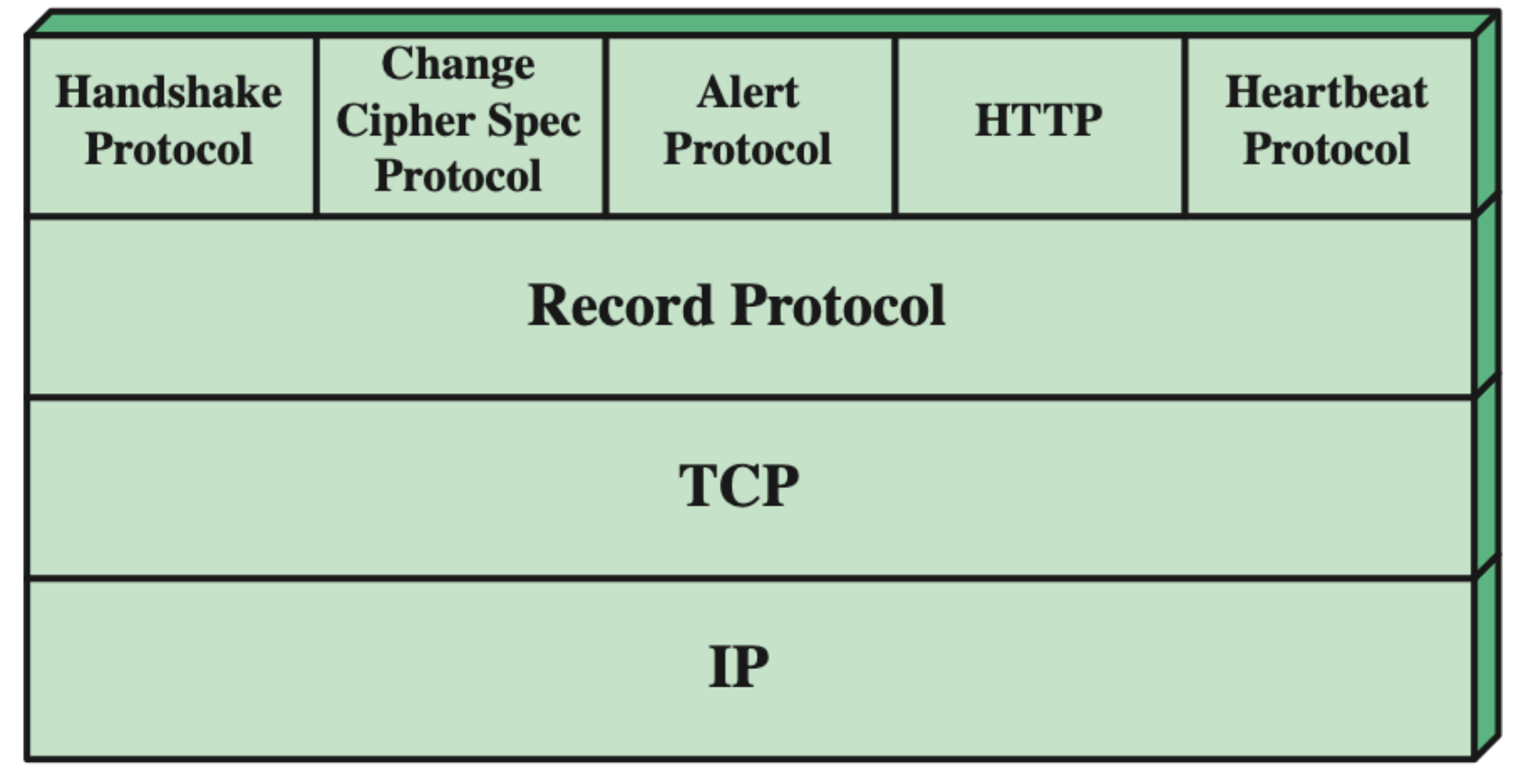
Odszyfrowanie i weryfikacja wiadomości.

SSL i TLS

SSl i TLS

SSL - Secure Sockets Layer
TLS - Transport Layer Security

- Najpowszechniej używane mechanizmy bezpieczeństwa
- Zestaw protokołów ogólnego przeznaczenia bazujących na protokole TCP
- SSL z czasem zostało przekształcone w TLS (RFC 4346)
- Mechanizmy mogą być implementowane jako składniki protokołów lub stosowane niezależnie



Stos protokołów TLS

TLS

Sesja - jest to powiązanie pomiędzy klientem a serwerem

- Sesje są tworzone za pomocą protokołu Handshake
- Sesje definiują zestaw kryptograficznych parametrów bezpieczeństwa, które mogą być współdzielone w wielu połączeniach
- Sesje wykorzystuje się w celu uniknięcia kosztownych negocjacji nowych parametrów bezpieczeństwa dla każdego połączenia.

TLS

- **Połączenie** — umożliwia transport (zgodnie z definicją modelu warstwowego OSI), który zapewnia odpowiedni rodzaj usługi. W przypadku TLS takie połączenia są relacjami peer-to-peer. Połączenia są krótkotrwałe. Każde połączenie jest powiązane z jedną sesją.

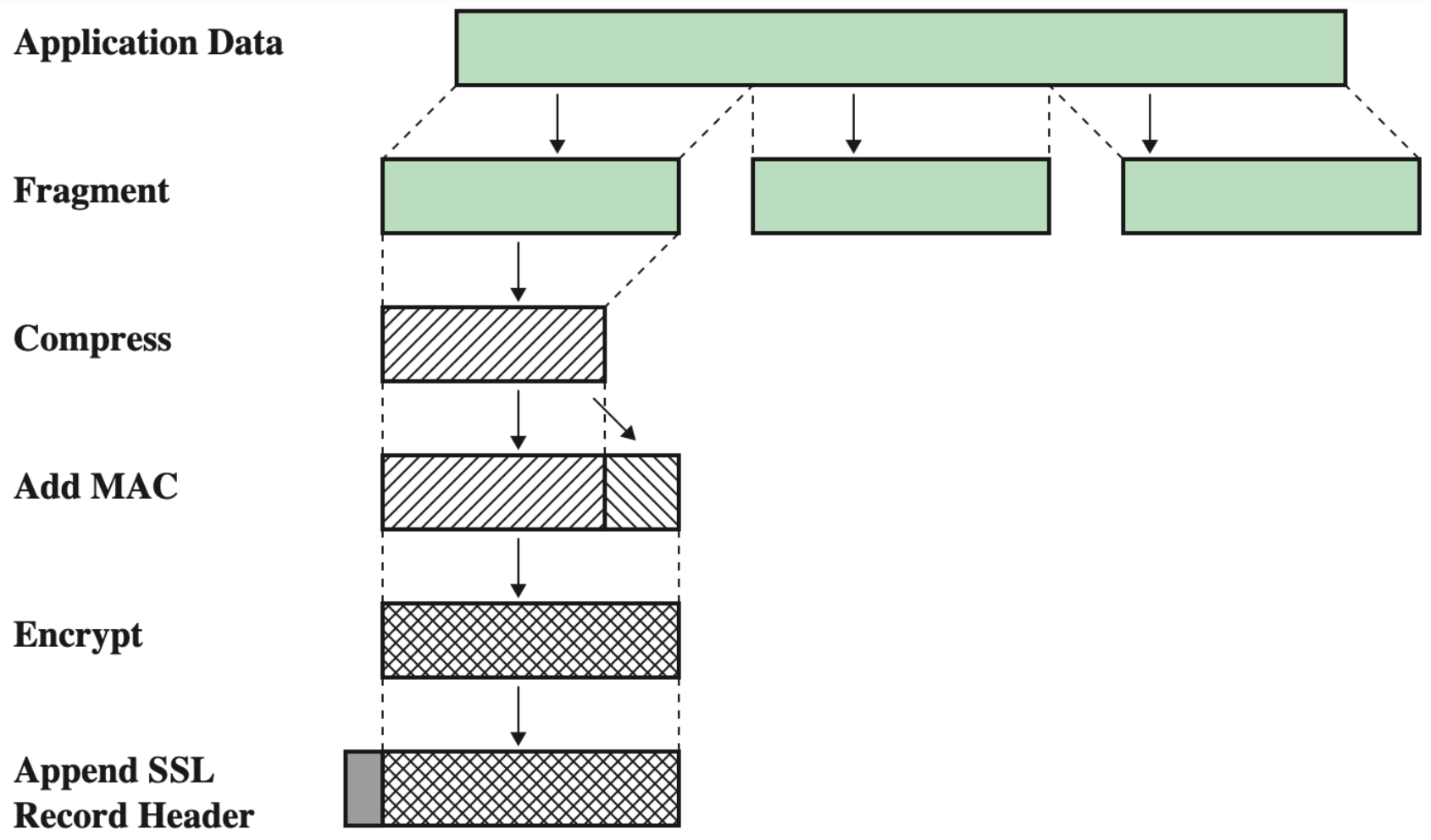
Protokoły TLS

Protokół Record (protokół SSL) zapewnia:

- poufność
- integralność

Podczas *Handshake* definiowane są klucze do symetrycznego szyfrowania ładunków oraz tajny klucz używany do tworzenia MAC.

Protokoły TLS



Dzianie protokołu TLS Record

Protokół Change Cipher Spec

- Jest najprostszy
- Składa się z jednej wiadomości składającej się z jednego bajtu o wartości 1
- Jedynym celem tej wiadomości jest spowodowanie skopiowania stanu oczekującego do stanu bieżącego
- Aktualizacja używanego zestawu szyfrów

Protokoły TLS

Protokół Alert - służy do przekazywania ostrzeżeń związanych z TLS do jednostki równorzędnej.
Składa się z dwóch bajtów:

- pierwszy bajt: **1** - ostrzeżenie, **2** - błąd krytyczny
- drugi bajt: kod komunikatu

Na przykład: Alert krytyczny: nieprawidłowy adres MAC
Alert niekrytyczny: `close_notify` (nadawca nie będzie wysyłał w tym połączeniu więcej komunikatów)

Protokoły TLS

Protokół **Handshake** umożliwia serwerowi i klientowi wzajemne uwierzytelnianie oraz negocjowanie algorytmu szyfrowania i MAC, wymianę kluczy kryptograficznych, które mają być używane do ochrony danych przesyłanych w rekordzie TLS.

Protokół *Handshake* jest wywoływany przed przesłaniem jakichkolwiek danych z użyciem TLS.

Protokoły TLS

Faza I
Wzajemne uwierzytelnianie

Faza II
Negocjacja algorytmu szyfrowania i MAC

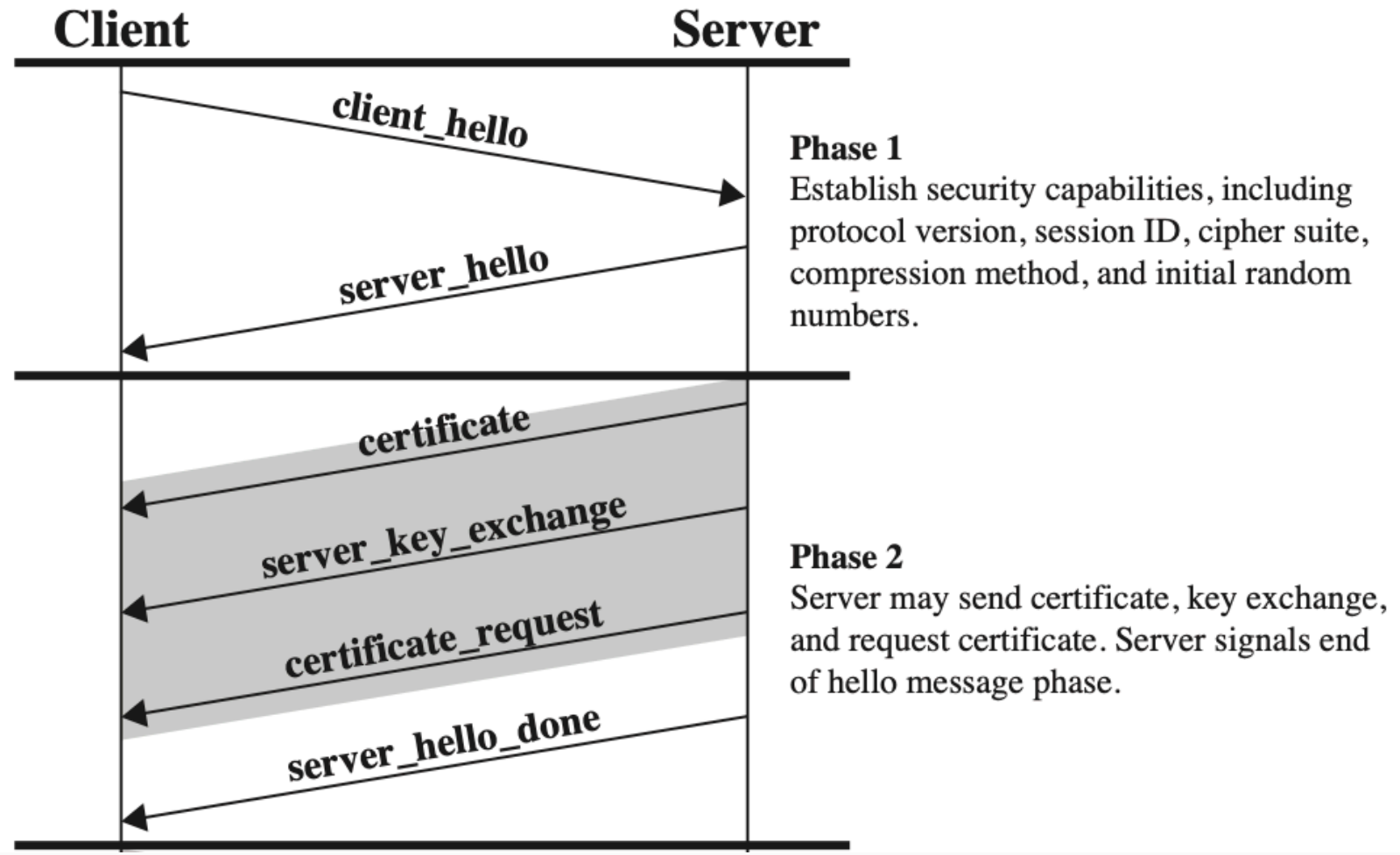
Faza III
Wymiana kluczy kryptograficznych

TLS Handshake

Szczegóły techniczne
Połączenie szyfrowane (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128-bitowe klucze, TLS 1.2)
Wyświetlana strona została zaszyfrowana przed przesłaniem poprzez Internet.

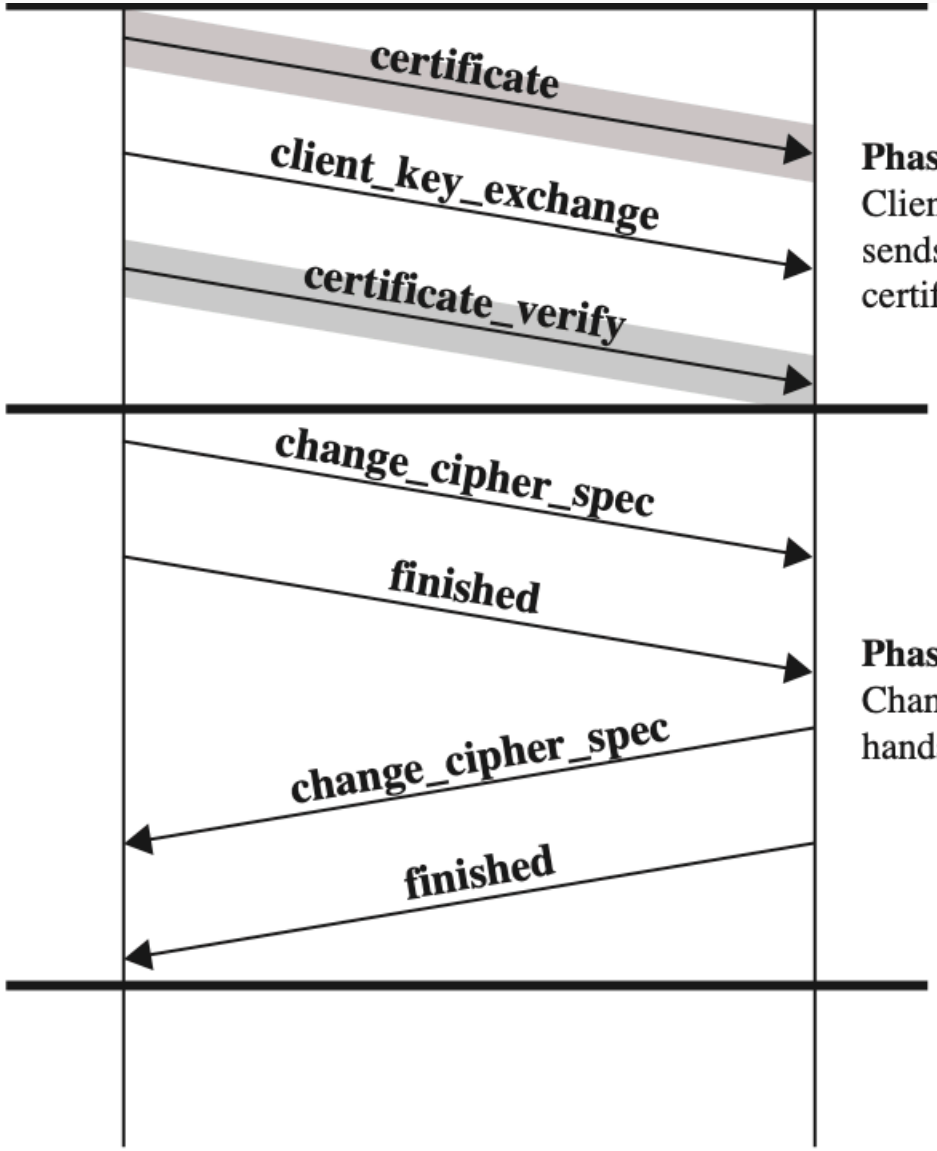
ECDHE	Elliptic Curve Diffie-Hellman Exchange - key exchange
RSA	Rivest-Shamir-Adleman Cryptosystem - public key authentication mechanism (for certificate verification)
AES_128_GCM	cipher_key size_Galois/Counter Mode encryption system
SHA256	hash function used for MAC

TLS Handshake



Działanie protokołu Handshake, cz. 1

TLS Handshake



Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Phase 4
Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

Działanie protokołu Handshake, cz. 2

TLS Heartbeat

Protokół **Heartbeat**:

- Okresowy sygnał generowany przez sprzęt lub oprogramowanie w celu wskazania normalnego działania lub synchronizacji z innymi częściami systemu
- Zwykle używany do monitorowania dostępności jednostki protokołu
- Zdefiniowany w 2012 roku w RFC 6250
- Działa w oparciu o protokół TLS Record, użycie jest ustalane podczas Fazy 1 protokołu Handshake (`heartbeat_request` i `heartbeat_response`).
- Każdy partner wskazuje, czy iw jaki sposób obsługuje ”bicie serca”

TLS Heartbeat

Protokół Heartbeat służy dwóm celom:

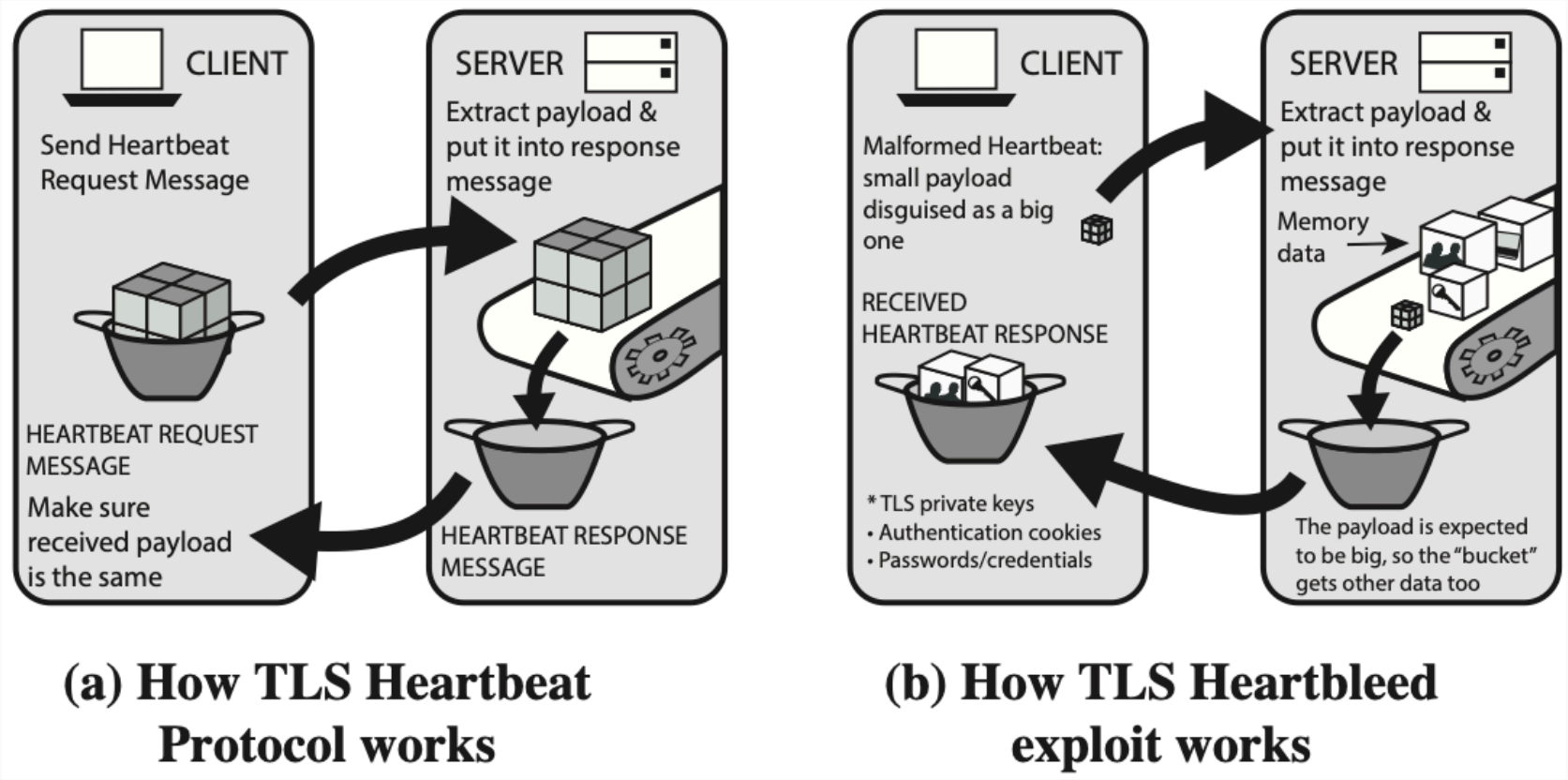
- Zapewnia nadawcę, że odbiorca ”żyje”
- Generuje aktywność w połączeniu w okresach bezczynności

Ataki na protokół TLS

Wektory ataku:

- Protokół Handshake
- Protokół Record i protokoły danych aplikacji
- PKI (Public Key Infrastructure)
- Inne

Heartbleed atak



Atak Heartbleed - exploit (źródło BAE Systems)

HTTPS

HTTPS

HTTPS - HTTP over SSL (port 443)

- Połączenie protokołu HTTP i SSL w celu wdrożenia bezpiecznej komunikacji między przeglądarką internetową a serwerem WWW
- Wbudowany we wszystkie nowoczesne przeglądarki internetowe (adresy URL zaczynają się od https://)
- Udokumentowane w RFC 2818, HTTP Over TLS
- Agent działający jako klient HTTP działa również jako klient TLS
- Zamknięcie połączenia HTTPS wymaga, aby TLS zamknęło połączenie z równorzędną jednostką TLS po stronie zdalnej, co będzie wiązało się z zamknięciem podstawowego połączenia TCP

HTTPS

Co jest szyfrowane:

- URL of the requested document
- Contents of the document
- Contents of browser forms (filled in by browser user)
- Cookies sent from browser to server and from server to browser
- Contents of HTTP header

HTTPS

https://google.pl

Szczegóły techniczne

Połączenie szyfrowane (TLS_AES_128_GCM_SHA256, 128-bitowe klucze, TLS 1.3)

https://pkobp.pl

Szczegóły techniczne

Połączenie szyfrowane (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128-bitowe klucze, TLS 1.2)

IPsec

IPsec

Dlaczego **IPsec**?

- Uwierzytelnianie - odebrany pakiet został faktycznie przesłany przez stronę zidentyfikowaną w nagłówku pakietu jako źródło (także integralność)
- Poufność - umożliwia komunikującym się węzłom szyfrowanie wiadomości w celu uniemożliwienia podsłuchania przez strony trzecie
- Zarządzanie kluczami - bezpieczeństwo wymiany kluczy

Aktualna wersja IPsec, określana jako IPsecv3, obejmuje uwierzytelnianie i poufność. Zarządzanie kluczami zapewnia standard **Internet Key Exchange** - IKEv2."

IPsec

Główną cechą protokołu IPsec, która umożliwia obsługę różnych aplikacji, jest jego funkcja szyfrowania i (lub) uwierzytelniania całego ruchu na poziomie IP. Dzięki temu można zabezpieczyć wszystkie aplikacje, w tym zdalne logowanie, aplikacje klient-serwer, pocztę e-mail, funkcję transferu plików, dostęp do sieci WWW i tym podobne.

IPsec

Gdy protokół IPsec jest zaimplementowany na zaporze lub w routerze, zapewnia ”solidne” zabezpieczenia, które można zastosować do całego z obszaru chronionego. Ruch z firmą lub grupą roboczą nie pociąga za sobą nakładów w przetwarzaniu związanym z bezpieczeństwem.

IPsec w firewall’u jest odporny na ominięcie, jeśli cały ruch z zewnątrz musi korzystać z protokołu IP, a firewall jest jedynym punktem gdzie ruch sieciowy wchodzi i wychodzi do organizacji.

IPsec

IPsec znajduje się ”poniżej” warstwy transportowej (TCP, UDP) i dlatego jest przezroczysty dla aplikacji. Nie ma potrzeby zmiany oprogramowania w systemie użytkownika lub serwera, jeśli protokół IPsec jest zaimplementowany w zaporze lub routerze. Nawet jeśli protokół IPsec jest zaimplementowany w systemach końcowych, nie ma to wpływu na oprogramowanie wyższej warstwy, w tym aplikacji.

IPsec

IPsec może być przezroczysty dla użytkowników końcowych. Nie ma potrzeby szkolenia użytkowników w zakresie mechanizmów bezpieczeństwa, wydawania materiałów dotyczących kluczy dla poszczególnych użytkowników ani unieważniania materiałów kluczy, gdy użytkownicy opuszczają organizację.

W razie potrzeby IPsec może zapewnić bezpieczeństwo indywidualnym użytkownikom. Jest to przydatne dla pracowników poza siedzibą firmy i do konfigurowania bezpiecznej wirtualnej podsieci w organizacji dla wrażliwych aplikacji.

IPsec

IPsec może także odgrywać kluczową rolę w architekturze routingu wymaganej w sieci.

- Ogłoszenie routera (nowy router ogłasza swoją obecność) pochodzi od autoryzowanego routera.
- Ogłoszenie sąsiada (router stara się nawiązać lub utrzymać relację sąsiada z routerem w innej domenie routingu) pochodzi z autoryzowanego routera.
- Komunikat przekierowania pochodzi z routera, do którego został wysłany pakiet początkowy.
- Aktualizacja routingu nie jest sfałszowana.

IPsec

Bez takich środków bezpieczeństwa atakujący może zakłócić komunikację lub przekierować część ruchu. Protokoły routingu, takie jak Open Shortest Path First (OSPF), powinny być uruchamiane na bazie powiązań zabezpieczeń między routerami zdefiniowanymi przez IPsec.

Asocjacje bezpieczeństwa

Asocjacje bezpieczeństwa:

Jednokierunkowa relacja między nadawcą a odbiorcą zapewniająca bezpieczeństwo ruchu.

Jeśli do dwukierunkowej bezpiecznej wymiany potrzebna jest relacja równorzędna, wymagane są dwie asocjacje

Jest jednoznacznie identyfikowana przez:

- SPI - Security Parameter Index
- IP - adres IP docelowy
- ESP lub AH - identyfikator protokołu

Prptpkoy IPsec

AH - Authentication Header - udostępnia funkcje uwierzytelniania (nieużywany w IPsec v3)

ESP - Encapsulating Security Payload - zapewnia usługi poufności, w tym poufność treści wiadomości i ograniczoną poufność przepływu ruchu. Opcjonalnie protokół ESP może również dostarczać usługi uwierzytelniania.

ESP

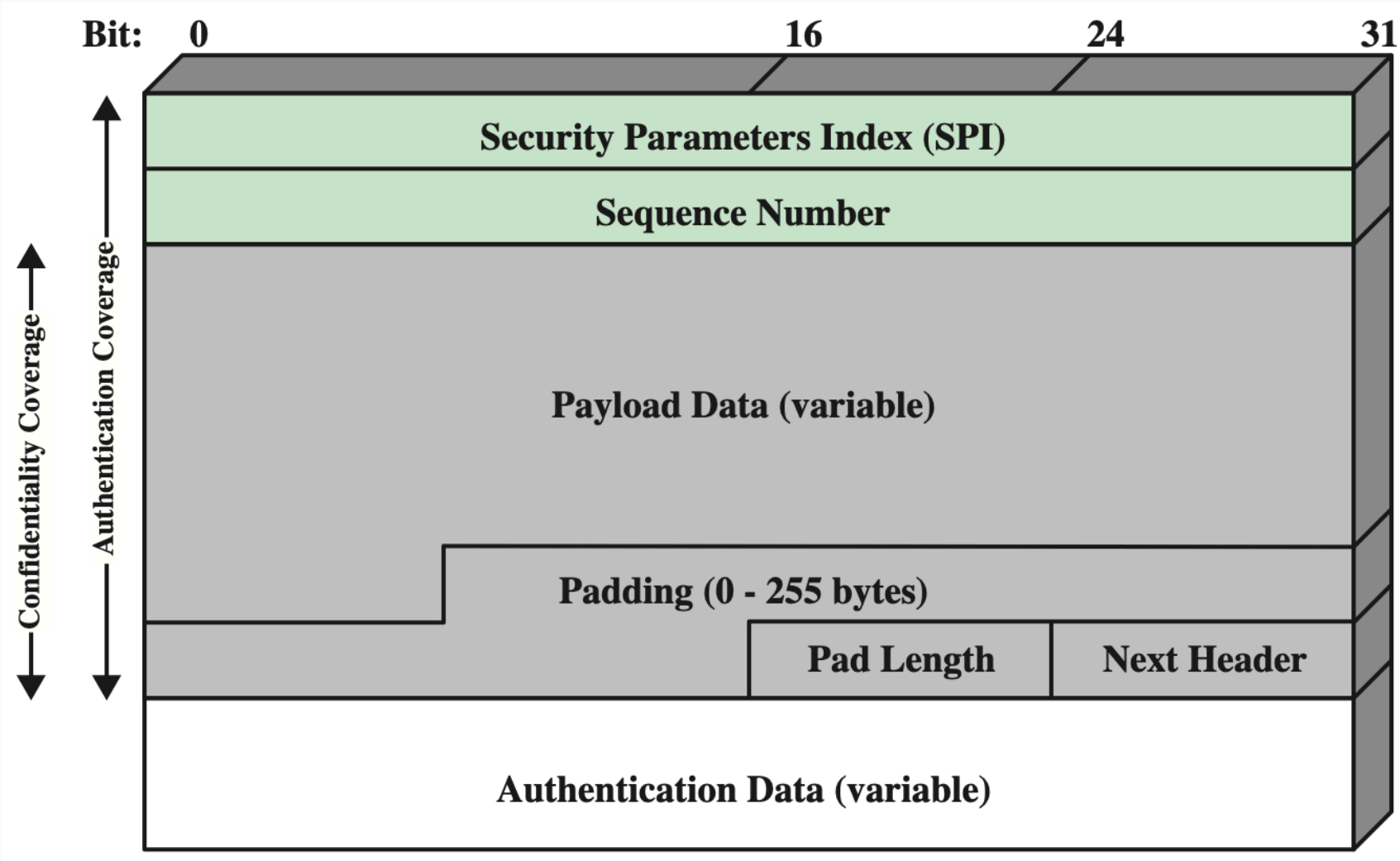
Pakiet ESP:

- Indeks SPI (32 bity) — identyfikuje asocjację bezpieczeństwa.
- Numer kolejny (32 bity) — monotonicznie rosnąca wartość licznika.
- Dane ładunku (zmienna) — segment poziomu transportu (tryb transportowy) lub pakiet IP (tryb tunelowy) chroniony przez szyfrowanie.
- Wypełnienie (0 – 255 bajtów) — może być konieczne, jeśli algorytm szyfrowania wymaga, aby tekst jawny był wielokrotnością pewnej liczby oktetów.
- Rozmiar wypełnienia (8 bitów) — wskazuje liczbę bajtów wypełnienia bezpośrednio poprzedzających to pole.

ESP

- Następny nagłówek (8 bitów) — określa typ danych zawartych w polu Dane ładunku poprzez identyfikację pierwszego nagłówka w tym ładunku (np. nagłówek rozszerzenia protokołu IPv6 lub protokół wyższej warstwy, taki jak TCP).
- Zmienna ICV (ang. Integrity Check Variable) — pole o zmiennej długości (musi być całkowitą liczbą 32-bitowych słów), które zawiera wartość sprawdzania integralności obliczoną dla pakietu ESP minus pole Dane uwierzytelniania.

ESP Frame§



Ramka protokołu ESP w IPsec

Tryby IPsec

Tryb transportowy - zapewnia ochronę przede wszystkim dla protokołów wyższych warstw:

- ochrona trybu transportowego rozciąga się na ładunek danych pakietu IP
- używany do komunikacji typu end-to-end pomiędzy dwoma hostami
- IPv4 - ładunek zwiera dane, które zwykle następują po nagłówku IP
- IPv6 - ładunek to dane, które zwykle występują za nagłówkiem IP oraz za wszystkimi nagłówkami rozszerzeń IPv6

ESP w trybie transportowym szyfruje i opcjonalnie uwierzytelnia ładunek danych IP, ale nie nagłówek IP.

Tryby IPsec

Tryb tunelowy - zapewnia ochronę całego pakietu IP, cały pakiet i pola zabezpieczeń są traktowane jako ładunek nowego zewnętrznego pakietu IP.

ESP w trybie tunelowym szyfruje i opcjonalnie uwierzytelnia cały wewnętrzny pakiet IP, w tym wewnętrzny nagłówek IP.

Dzięki trybowi tunelowemu jest możliwe tworzenie wirtualnych sieci prywatnych (VPN), które stanowią główne zastosowanie IPsec.

Bezpieczeństwo systemów operacyjnych

Marek Miśkiewicz

wykład 4

Uwierzytelnianie w sieci Internet

Kerberos

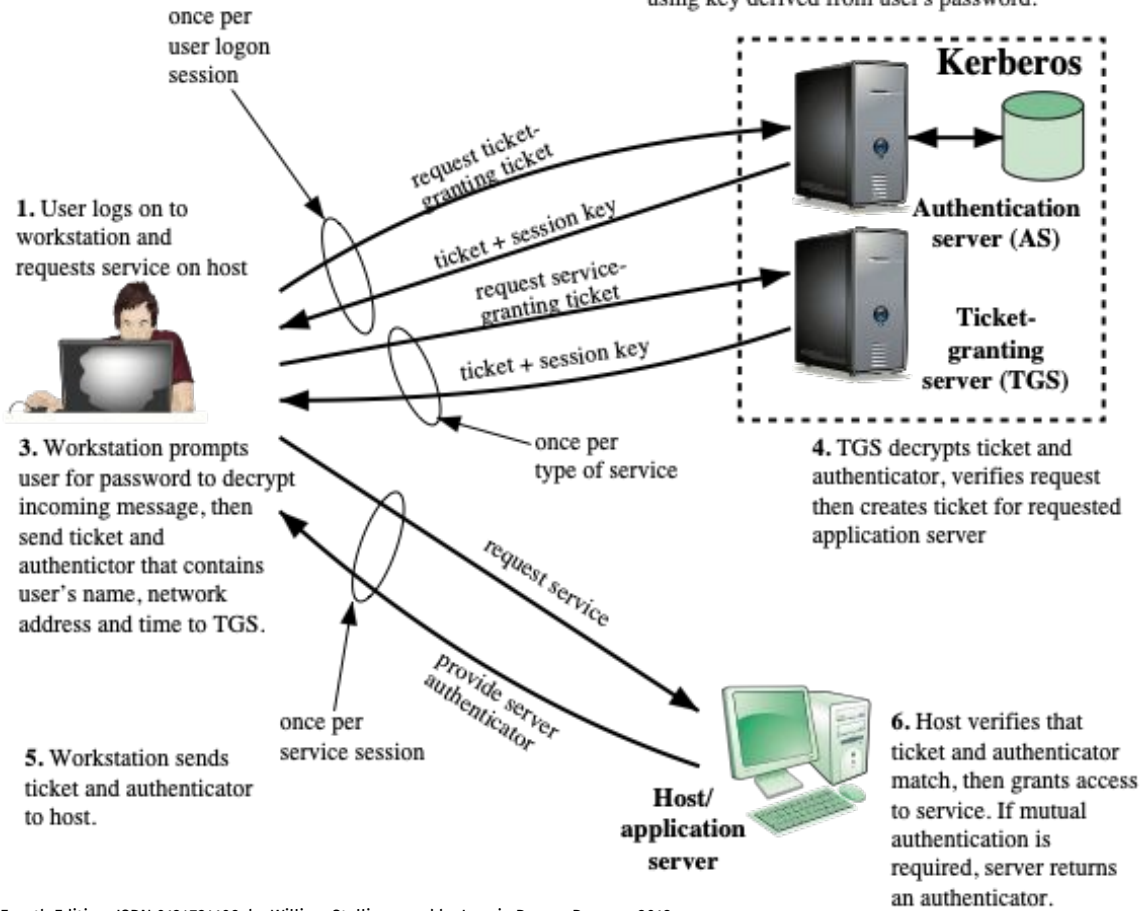
Kerberos

- Początkowo opracowany w MIT
- Narzędzie programowe dostępne zarówno w domenie publicznej, jak i w wersje obsługiwane komercyjnie
- Wydany jako standard internetowy i jest standardem defacto dla zdalnego uwierzytelniania
- Do uwierzytelniania wykorzystywana jest zaufana trzecia strona (Third Party)
- Wymaga, aby użytkownik udowodnił swoją tożsamość dla każdej wywoływanej usługi i wymaga, aby serwery udowodniły swoją tożsamość klientom

Kerberos - protokół

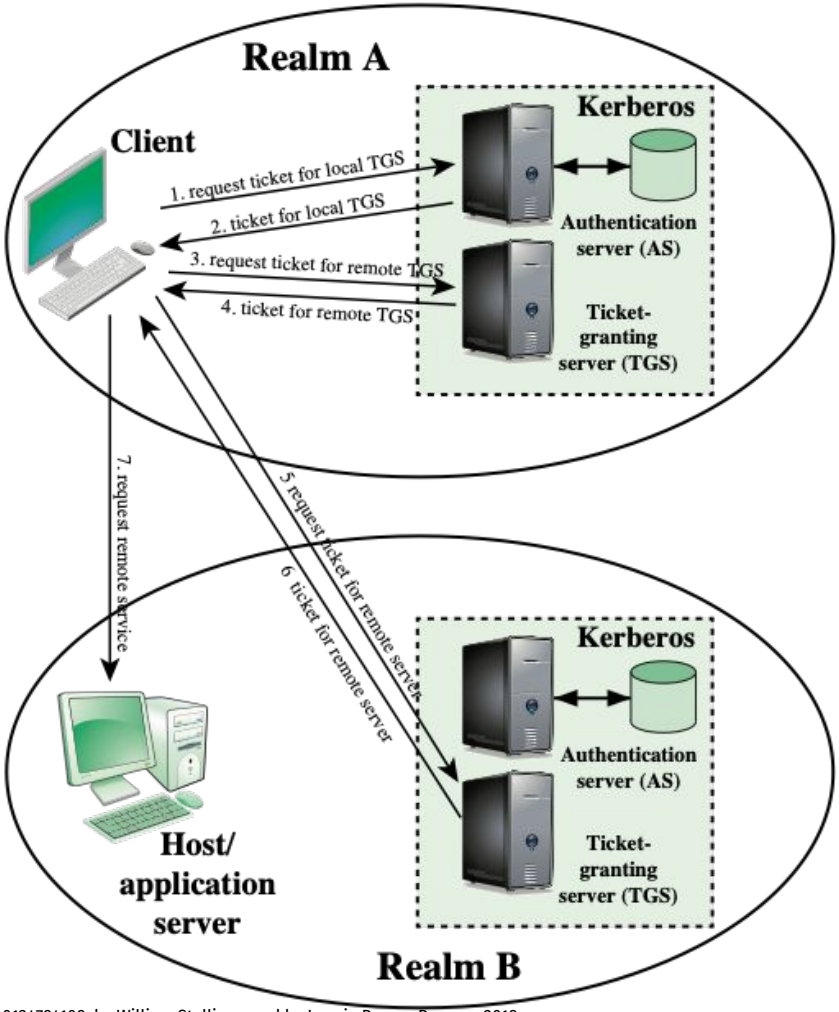
- Obejmuje klientów, serwery aplikacji i serwer Kerberos
  - Zaprojektowany, aby przeciwdziałać różnorodnym zagrożeniom dla bezpieczeństwa dialogu klient / serwer.
  - Oczywistym zagrożeniem dla bezpieczeństwa jest podszywanie się.
  - Serwery muszą mieć możliwość potwierdzania tożsamości klientów żądających usługi.
- Authentication Server (AS)
  - Użytkownik początkowo negocjuje z AS w celu weryfikacji tożsamości
  - AS weryfikuje tożsamość, a następnie przekazuje informacje do serwera aplikacji, który następnie przyjmuje żądania usług od klienta

Trzeba to zrobić w bezpieczny sposób: Jeśli klient wyśle hasło użytkownika do AS przez sieć, atakujący może je zauważyć. Atakujący może podszywać się pod AS i wysłać fałszywe potwierdzenie.


2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
once per user logon session
Kerberos
request ticket-granting ticket
ticket + session key
Authentication server (AS)
1. User logs on to workstation and requests service on host
request service-granting ticket
ticket + session key
Ticket-granting server (TGS)
once per type of service
3. Workstation prompts user for password to decrypt incoming message, then send ticket and authentictor that contains user's name, network address and time to TGS.
4. TGS decrypts ticket and authenticator, verifies request then creates ticket for requested application server
request service
provide server authenticator
once per service session
5. Workstation sends ticket and authenticator to host.
Host/ application server
6. Host verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

Domena Kerberosa

- Środowisko Kerberosa:
  - Serwer Kerberos
  - Klienci, wszyscy zarejestrowani na serwerze
  - Serwery aplikacji współdzielące klucze z serwerem
- Domeny - sieci klientów i serwerów w ramach różnych organizacji
- W przypadku wielu współdziałających domen serwery Kerberos muszą ufać sobie nawzajem


Realm A
Client
Kerberos
1. request ticket for local TGS
2. ticket for local TGS
3. request ticket for remote TGS
4. ticket for remote TGS
Authentication server (AS)
Ticket-granting server (TGS)
7. request remote service
5 request ticket for remote server
6 ticket for remote server
Host/ application server
Kerberos
Authentication server (AS)
Ticket-granting server (TGS)
Realm B

Kerberos - wersja 5

- Pierwszą szeroko stosowaną wersją protokołu Kerberos była wersja 4, opublikowana pod koniec lat 80
- Ulepszenia w wersji 5:
  - Zaszyfrowana wiadomość jest oznaczona identyfikatorem algorytmu szyfrowania Umożliwia to użytkownikom skonfigurowanie protokołu Kerberos do korzystania z algorytmu innego niż DES
  - Obsługuje przekazywanie uwierzytelniania
    - Umożliwia klientowi dostęp do serwera i umożliwia temu serwerowi dostęp do innego serwera w imieniu klienta
    - Obsługuje metodę uwierzytelniania między obszarami, która wymaga mniejszej liczby bezpiecznych wymian kluczy niż w wersji 4

Kerberos - problemy wydajnościowe

- Problem rozmiaru środowiska klient-serwer
- Dla rozległych środowisk jeśli system jest poprawnie skonfigurowany, to wpływ stosowania protokołu Kerberos na wydajność jest niewielki
- Najlepszym sposobem zapewnienia bezpieczeństwa protokołu Kerberos jest umieszczenie serwera Kerberos na oddzielnym, odizolowanym komputerze
- Wiele oddzielnych domen to wymóg raczej geograficzny niż sprzętowy

Urzędy certyfikacji

Urzędy certyfikacji - CA

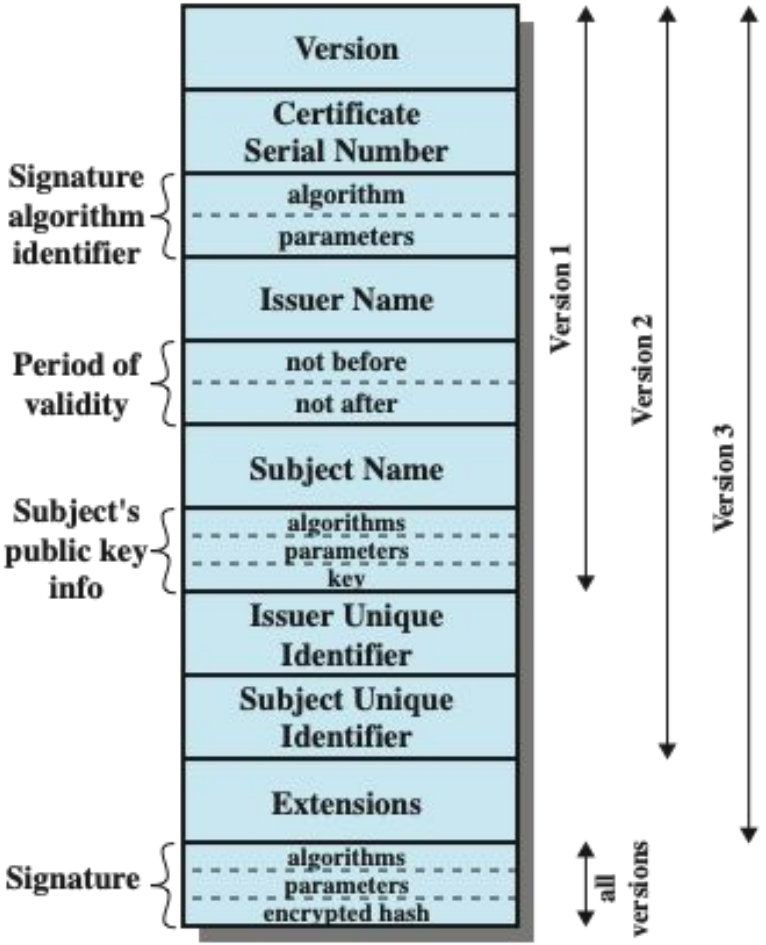
W skład certyfikatu w ogólności wchodzi:

- klucz publiczny właściciela (dokładnie określona tożsamość)
- podpis zaufanej trzeciej strony (TTP) - wystawcy certyfikatu

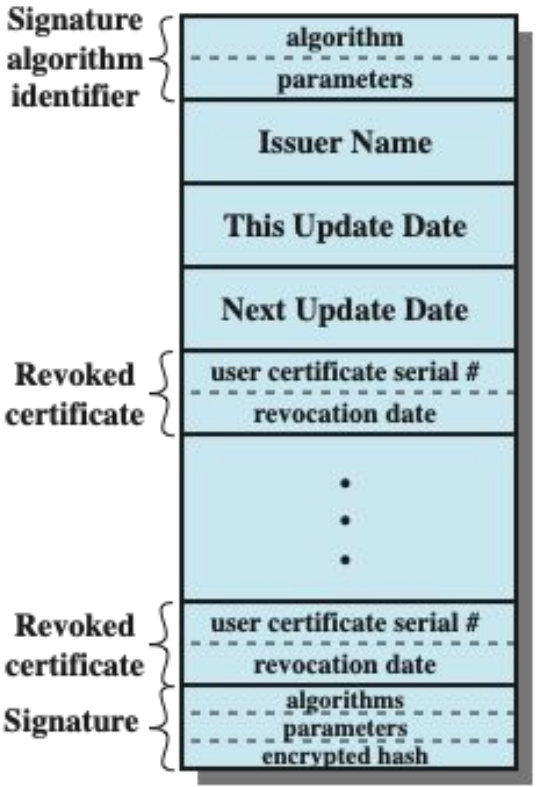
Zazwyczaj stroną trzecią jest CA, któremu ufają społeczności użytkowników (takie jak agencja rządowa, firma telekomunikacyjna, instytucja finansowa lub inna zaufana organizacja). Użytkownik może w bezpieczny sposób przedstawić urzędowi swój klucz publiczny i uzyskać certyfikat. Użytkownik może następnie opublikować certyfikat lub wysłać go innym. Każdy, kto potrzebuje klucza publicznego tego użytkownika, może uzyskać certyfikat i zweryfikować jego ważność za pomocą dołączonego zaufanego podpisu.

Standard X.509

Standard **ITU-T X.509**, określony również w specyfikacji RFC 5280, jest najpowszechniej akceptowanym formatem certyfikatów klucza publicznego. Certyfikaty X.509 są używane w większości aplikacji zabezpieczających sieć, w tym w zabezpieczeniach IP Security (IPSEC), SSL (ang. Secure Socket Layer), TLS (ang. Transport Layer Security), SET (ang. Secure Electronic Transactions) i S/MIME, a także w aplikacjach eBusiness.



(a) X.509 Certificate



(b) Certificate Revocation List

Rodzaje certyfikatów

- Certyfikaty konwencjonalne
  - Certyfikaty CA i „użytkowników końcowych”
  - Zwykle wydawane na okresy ważności od miesięcy do lat
- Certyfikaty krótkotrwałe
  - Służy do zapewniania uwierzytelniania w aplikacjach, takich jak przetwarzanie sieciowe, przy jednoczesnym uniknięciu niektórych kosztów ogólnych i ograniczeń konwencjonalnych certyfikatów
  - Mają okresy ważności od godzin do dni, co ogranicza okres niewłaściwego użycia w przypadku naruszenia
  - Ponieważ zwykle nie są wydawane przez uznane CA, istnieją problemy z weryfikacją ich poza ich organizacją wydającą

Rodzaje certyfikatów

- Certyfikaty proxy
  - Powszechnie stosowany do zapewniania uwierzytelniania w aplikacjach, takich jak przetwarzanie sieciowe, przy jednoczesnym uwzględnieniu niektórych ograniczeń krótkoterminowych certyfikatów
  - Identyfikowane przez obecność rozszerzenia „certyfikatu proxy”
  - Pozwalają one certyfikatowi „użytkownika końcowego” na podpisanie innego certyfikatu
  - Umożliwiają one użytkownikowi łatwe tworzenie poświadczeń umożliwiających dostęp do zasobów w określonym środowisku bez konieczności podawania pełnego certyfikatu i uprawnień

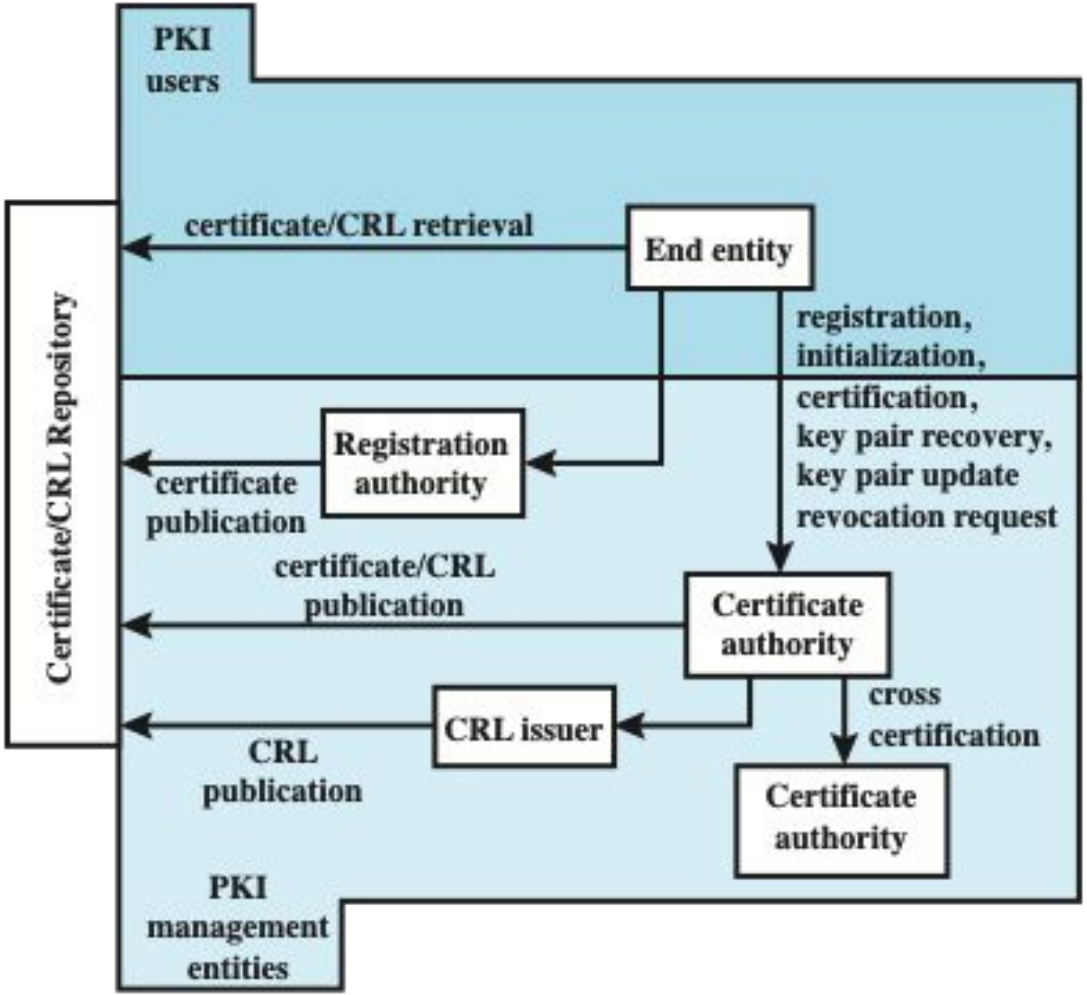
Rodzaje certyfikatów

- Certyfikaty atrybutów
  - Używają innego formatu certyfikatu, aby połączyć tożsamość użytkownika z zestawem atrybutów, które są zwykle używane do autoryzacji i kontroli dostępu
  - Użytkownik może mieć wiele różnych certyfikatów atrybutów, z różnymi zestawami atrybutów do różnych celów
  - Zdefiniowane w rozszerzeniu „Atrybuty”

Infrastruktura klucza publicznego

Infrastruktura klucza publicznego

- Zestaw sprzętu, oprogramowania, ludzi, zasad i procedur niezbędnych do tworzenia, zarządzania, przechowywania, dystrybucji i unieważniania certyfikatów cyfrowych w oparciu o kryptografię asymetryczną
- Opracowany, aby umożliwić bezpieczne, wygodne i wydajne pozyskiwanie kluczy publicznych
- „Trusted Store”
  - Lista urzędów certyfikacji i ich kluczy publicznych


PKI
users
certificate/CRL retrieval
End entity
registration,
initialization,
certification,
key pair recovery,
key pair update
revocation request
Certificate/CRL Repository
Registration
authority
certificate
publication
certificate/CRL
publication
Certificate
authority
cross
certification
CRL issuer
CRL
publication
Certificate
authority
PKI
management
entities

Bezpieczeństwo sieci bezprzewodowych

Bezpieczeństwo sieci bezprzewodowych

Kluczowe czynniki wpływające na większe ryzyko bezpieczeństwa sieci bezprzewodowych w porównaniu z sieciami przewodowymi to:

- Kanał
  - Sieci bezprzewodowe zazwyczaj obejmują komunikację rozgłoszeniową, która jest znacznie bardziej podatna na podsłuchiwanie i zagłuszanie niż sieci przewodowe
  - Sieci bezprzewodowe są również bardziej podatne na aktywne ataki, które wykorzystują luki w protokołach komunikacyjnych
- Mobilność
  - Urządzenia bezprzewodowe są znacznie bardziej przenośne i mobilne, co wiąże się z szeregiem zagrożeń

Bezpieczeństwo sieci bezprzewodowych

- Zasoby
  - Niektóre urządzenia bezprzewodowe, takie jak smartfony i tablety, mają wyrafinowane systemy operacyjne, ale mają ograniczoną pamięć i zasoby przetwarzania, do tego aby przeciwdziałać zagrożeniom i złośliwemu oprogramowaniu
- Dostępność
  - Niektóre urządzenia bezprzewodowe, takie jak sensory i roboty, mogą pozostać bez nadzoru w odległych i / lub wrogich lokalizacjach, co znacznie zwiększa ich podatność na ataki fizyczne

Bezpieczeństwo sieci bezprzewodowych

Zagrożenia w sieciach bezprzewodowych:

- Przypadkowe połączenie
- Złośliwe połączenie
- Sieci *ad hoc*
- Sieci nietradycyjne
- Kradzież tożsamości (podszywanie się pod MAC)
- Ataki *man-in-the-middle*
- Denial of service
- Iniekcje sieci

Sieci bezprzewodowe - środki bezpieczeństwa

Zabezpieczanie transmisji bezprzewodowych:

- Techniki ukrywania sygnału
  - utrudnienia atakującemu zlokalizowania punktów dostępu bezprzewodowego
  - wyłączenie nadawania przez bezprzewodowe punkty dostępowe identyfikatorów SSID
  - nadawanie identyfikatorom SSID kryptycznych nazw
  - zmniejszenie siły sygnału do najniższego poziomu, zapewniającego wymagane pokrycie
  - zlokalizowanie punktów dostępu bezprzewodowego wewnątrz budynków, z dala od okien i ścian zewnętrznych;
  - zastosowanie anten kierunkowych i technik osłaniania sygnału.
- Szyfrowanie

Sieci bezprzewodowe - środki bezpieczeństwa

Wykorzystanie protokołów **szyfrowania** i uwierzytelniania jest standardową metodą przeciwdziałania próbom modyfikowania lub wstawek do transmisji.

Sieci bezprzewodowe - środki bezpieczeństwa

Zabezpieczanie sieci bezprzewodowych

- Stosuj szyfrowanie
- Używaj oprogramowania antywirusowego i antyszpiegowskiego oraz zapór firewall
- Wyłącz rozgłaszanie identyfikatorów
- Zmień identyfikator routera z domyślnego
- Zmień domyślne hasło administratora routera
- Zezwalaj na dostęp do Twojej sieci bezprzewodowej tylko określonym komputerom (MAC)

Sieci bezprzewodowe - środki bezpieczeństwa

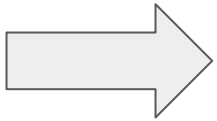
Zabezpieczanie bezprzewodowych punktów dostępowych

- Głównym zagrożeniem związanym z punktami dostępu bezprzewodowego jest nieautoryzowany dostęp do sieci
- Głównym podejściem do zapobiegania takiemu dostępowi jest standard IEEE 802.1X dotyczący kontroli dostępu do sieci w oparciu o porty
- Standard zapewnia mechanizm uwierzytelniania dla urządzeń, które chcą podłączyć się do sieci LAN lub sieci bezprzewodowej
- Korzystanie ze standardu 802.1X może zapobiec sytuacji, w której fałszywe punkty dostępowe i inne nieautoryzowane urządzenia staną się niebezpiecznymi backdoorami

Bezpieczeństwo urządzeń mobilnych

Zmiana paradygmatu

Bezpieczeństwo komputerów i sieci w firmach



Elementy rozproszone

Zmiana paradygmatu

Co należy uwzględniać:

- Rosnące wykorzystanie nowych urządzeń
- Aplikacje w chmurze
- Deperymetryzacja
- Zewnętrzne wymagania biznesowe

Urządzenia mobilne - zagrożenia

W dokumencie NIST SP 800-124 (Guidelines for Managing the Security of Mobile Devices in the Enterprise, czerwiec 2013 r.) wyszczególniono siedem poważnych problemów bezpieczeństwa dotyczących urządzeń mobilnych

- Brak zabezpieczeń fizycznych
- Używanie niezuafanych urządzeń mobilnych
- Korzystanie z niezufanych sieci
- Korzystanie z niezufanych aplikacji
- Interakcje z innymi systemami
- Korzystanie z niezuafanych treści
- Korzystanie z usług lokalizacyjnych

Urządzenia mobilne - zagrożenia

Bezpieczeństwo urządzeń:

- Dział IT weryfikuje każde urządzenie (BYOD) (root'ed, jail-broken)
- Włączenie automatycznego blokowania
- Włączenie ochrony hasłem lub kodem PIN
- Unikanie używania funkcji autouzupełniania do zapamiętywania nazw użytkowników lub haseł
- Włączenie zdalnego czyszczenia
- Zadbanie o to, aby była włączona ochrona SSL, jeśli jest dostępna
- Zadbanie o aktualizację oprogramowania, w tym systemów operacyjnych i aplikacji
- Zainstalowanie oprogramowania antywirusowego, gdy tylko stanie się dostępne
- Możliwość zdalnego dostępu do urządzeń, usuwania z nich wszystkich danych
- Polityka bezpieczeństwa może wymagać, aby usługa lokalizacji była wyłączona na wszystkich urządzeniach mobilnych

Urządzenia mobilne - zagrożenia

Bezpieczeństwo ruchu:

- Cały ruch powinien być szyfrowany i przekazywany za pomocą bezpiecznych protokołów (SSL, IPv6, VPN)
- Preferowaną strategią jest posiadanie dwuwarstwowego mechanizmu uwierzytelniania, który obejmuje uwierzytelnianie urządzenia, a następnie uwierzytelnianie jego użytkownika.

Bezpieczeństwo granic:

- Organizacja powinna posiadać mechanizmy bezpieczeństwa mające na celu ochronę sieci przed nieautoryzowanym dostępem. Strategia bezpieczeństwa może również obejmować reguły zapór firewall specyficzne dla ruchu urządzeń mobilnych.

Standard IEEE 802.11

IEEE 802 jest komitetem, który opracował standardy dla dużej gamy sieci lokalnych (LAN). W 1990 r. komitet ten utworzył nową grupę roboczą o nazwie IEEE 802.11, której zadaniem było opracowania protokołu i specyfikacji transmisji dla bezprzewodowych sieci LAN (WLAN). Z czasem zapotrzebowanie na sieci WLAN o różnych częstotliwościach i szybkościach transmisji danych gwałtownie wzrosło. Starając się nadążyć za tym zapotrzebowaniem, grupa robocza IEEE 802.11 opublikowała listę standardów, która stale się rozszerza.

Standard IEEE 802.11

Terminologia IEEE 802.11

Punkt dostępowy (ang. access point — AP)	Dowolny podmiot, który ma funkcjonalność stacji roboczej i zapewnia dostęp do systemu dystrybucyjnego dla powiązanych stacji za pośrednictwem bezprzewodowego medium
Podstawowy zestaw usług (ang. basic service set — BSS)	Zestaw stacji sterowanych za pomocą pojedynczej funkcji koordynacji
Funkcja koordynacji	Funkcja logiczna, która określa, kiedy stacja działająca w ramach BSS może transmitować i odbierać jednostki danych PDU
System dystrybucji (ang. distribution system — DS)	System służący do połączenia zbioru systemów BSS i zintegrowanych sieci LAN w celu utworzenia systemu ESS
Rozszerzony zestaw usług (ang. extended service set — ESS)	Zbiór złożony z jednego lub większej liczby wzajemnie połączonych BSS i zintegrowanych sieci LAN, które dla warstwy LLC są widoczne z dowolnej stacji powiązanej z jednym z tych BSS jako jeden BSS

Standard IEEE 802.11

Terminologia IEEE 802.11

Jednostka danych protokołu MAC (ang. MAC protocol data unit — MPDU)	Jednostka danych wymieniana pomiędzy dwoma równorzędnymi jednostkami MAC korzystającymi z usług warstwy fizycznej
Jednostka usług protokołu MAC (ang. MAC service data unit — MSDU)	Informacje dostarczane pomiędzy użytkownikami MAC jako jednostka
Stacja	Dowolne urządzenie posiadające adres MAC zgodny z IEEE 802.11 i warstwę fizyczną

Na podstawie: William Stallings, Lawrie Brown, *Computer Security: Principles and Practice (4th Edition)*, Helion 2019

IEEE 802.11

- Pierwszy standard z szeroką akceptacją - 802.11b
- W roku 1999 powstaje konsorcjum branżowe Wireless Ethernet Compatibility Alliance (WECA)
- Z biegiem czasu zostaje przemianowane na Wi-Fi Alliance (Wireless Fidelity) i tworzy zestaw certyfikacyjny Wi-Fi (802.11b) -> 802.11g -> 802.11a
- Wi-Fi Alliance opracowała procedury certyfikacji dla standardów bezpieczeństwa IEEE 802.11, określane jako Wi-Fi Protected Access (WPA). **Nie** najnowsza wersja WPA, znana jako WPA2, zawiera wszystkie funkcje specyfikacji zabezpieczeń WLAN IEEE 802.11i. -> WPA3

Bezpieczeństwo systemów operacyjnych

Marek Miśkiewicz

wykład 5

Malware

Terminologia

APT (advanced persistent threat) - Cyberprzestępczość (przestępczość komputerowa) wymierzona w cele gospodarcze lub polityczne z zastosowaniem szerokiej gamy technik włamaniowych i malware'u, charakteryzująca się uporczywością i efektywnością ataków na umyślne cele przez długie okresy, często wymierzona przeciw instytucjom subsydiowanym przez państwo.

Adware (advertising-supported software) - Reklama scalona z oprogramowaniem. Może powodować wyskakiwanie dodatków reklamowych lub przekierowywanie przeglądarki na witryny handlowe.

Attack Kit - Zestaw narzędzi do generowania nowego malware'u, automatycznie wykorzystującego rozmaite załączone mechanizmy rozsiewania i obciążania ładunkami.

Terminologia

Auto-rooter - Wrogie narzędzia hakerskie, używane do zdalnych włamań do nowych maszyn.

Backdoor - Każdy mechanizm omijający zwykłą kontrolę bezpieczeństwa; może skutkować nieupoważnionym dostępem do funkcji w programie lub w zaatakowanym (pozbawionym ochrony) systemie.

Downloader - Kod instalujący inne jednostki na zaatakowanej maszynie. Zwykle dołączany do kodu malware'u wstawianego najpierw do obezwładnianego systemu, a potem importującego większy pakiet szkodliwego oprogramowania.

Terminologia

Drive-by-download - Atak z użyciem kodu na opanowanej witrynie, który wykorzystuje słaby punkt w przeglądarce do napaści na system klienta podczas przeglądania odwiedzanej witryny,

Exploit - Kod ukierunkowany na konkretną słabość lub zbiór słabości

Flooders - Używane do generowania wielkich ilości danych w celu atakowania sieciowych systemów komputerowych przez realizowanie pewnej odmiany ataku typu „odmowa świadczenia usług” (DoS).

Keylogger - Przechwytują naciskanie klawiszy klawiatury w zaatakowanym systemie.

Terminologia

Logic-bomb - Kod wstawiony do malware'u przez intruza. Bomba logiczna spoczywa uśpiona aż do wystąpienia z góry określonego warunku; wówczas kod powoduje uruchomienie jakiegoś ładunku

Macro virus - Rodzaj wirusa używającego makrodefinicji lub kodu skryptowego, zwykle wbudowanego w dokument lub szablon dokumentu, uaktywniającego się podczas oglądania lub redagowania dokumentu w celu wykonania i zreplikowania się w innych takich dokumentach.

Mobile code - Oprogramowanie (np. skrypt lub makrodefinicja), które może być wysłane w niezmienionej postaci na platformy różnych typów i działać tam z identyczną semantyką.

Terminologia

Rootkit - Zestaw narzędzi hakerskich używany po włamaniu się napastnika do systemu komputerowego i uzyskaniu dostępu na poziomie administratora („roota”)

Spammer programs - Używane do wysyłania wielkich ilości niepożądanej poczty

Spyware - Oprogramowanie zbierające informacje z komputera i przesyłające je do innego systemu w drodze monitorowania naciśnięć klawiszy, danych wyświetlanych na ekranie i (lub) ruchu sieciowego, względnie skanujące pliki systemu w poszukiwaniu wrażliwych informacji.

Terminologia

Trojan horse - Program komputerowy udający użyteczną funkcję, lecz skrywający również funkcję potencjalnie groźną, która omija mechanizmy bezpieczeństwa, niekiedy wykorzystując legalne upoważnienia jednostki systemowej, która go wywołała

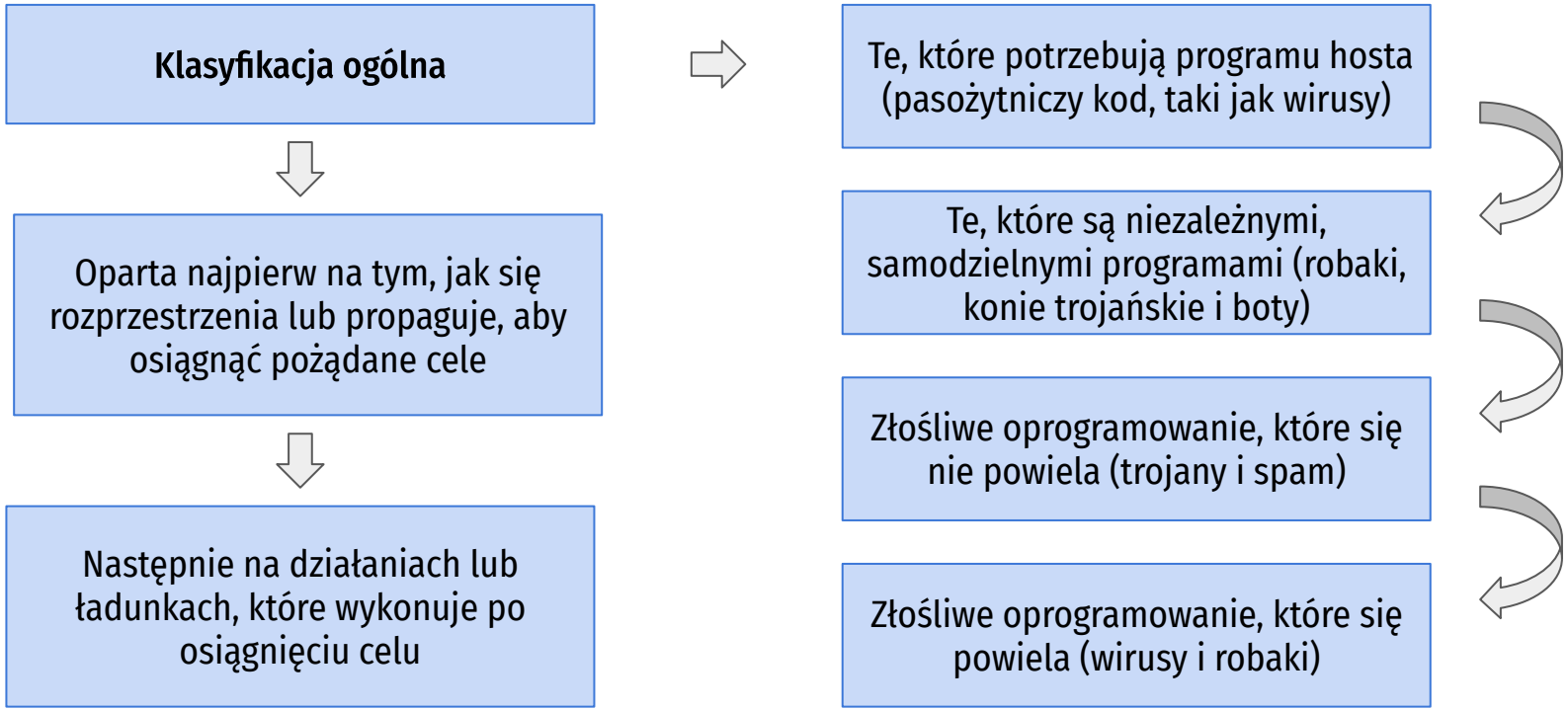
Virus - Wredne oprogramowanie, które — uruchomione — próbuje się rozmnożyć na innej działającej maszynie lub w kodzie skryptowym. O kodzie, w którym to się powiodło, mówi się, że został zainfekowany. Jeśli zainfekowany kod jest wykonywany, wirus jest również wykonywany

Worm - Program komputerowy potrafiący działać niezależnie i rozsiewać kompletną, działającą wersję samego siebie na innych komputerach w sieci, wykorzystując słabości oprogramowania w docelowym systemie lub przechwycone poświadczenia upoważnień

Terminologia

Zombie, bot - Program zainstalowany w zainfekowanej maszynie, który uaktywnia się w celu przypuszczania ataków na inne maszyny.

Malware - klasyfikacja



Attack Kits

- Początkowo tworzenie i wdrażanie złośliwego oprogramowania wymagało od autorów oprogramowania znacznych umiejętności technicznych
  - Rozwój zestawów narzędzi do tworzenia wirusów na początku lat 90. XX wieku, a następnie bardziej ogólnych zestawów do ataku na początku XXI wieku, znacznie pomógł w opracowywaniu i wdrażaniu złośliwego oprogramowania
- Zestawy narzędzi są często znane jako „crimeware”
  - Uwzględnij różnorodne mechanizmy propagacji i moduły ładunku, które mogą wdrożyć nawet nowicjusze
  - Warianty, które mogą być generowane przez osoby atakujące za pomocą tych zestawów narzędzi, stanowią poważny problem dla osób broniących się przed nimi systemów
- Przykłady:
  - Zeus
  - Angler

Źródła ataku

Motywacja polityczna

Bezpośredni zysk

Przestępstwa i przestępczość zorganizowana

Agencje państwowe

Znaczącym powodem dla rozwoju złośliwego oprogramowania jest zmiana motywacji do zademonstrowania swoich kompetencji technicznych swoim rówieśnikom na bardziej zorganizowane i niebezpieczne źródła ataków.

Sytuacja ta spowodowała znaczną zmianę dostępnych zasobów i motywację do powstania złośliwego oprogramowania, przez co doprowadziło do rozwoju dużej szarej strefy obejmującej sprzedaż zestawów atakujących, dostęp do zainfekowanych hostów i skradzionych informacji.

Advanced Persistent Threats

- Dobrze wyposażone, trwałe stosowanie szerokiej gamy technologii włamań i złośliwego oprogramowania do wybranych celów (zwykle biznesowych lub politycznych)
- Zwykle przypisywany organizacjom sponsorowanym przez państwo i przedsiębiorstwom przestępczym
- Różnią się od innych typów ataków starannym wyborem celu i ukrywaniem się przez dłuższy czas
- Ataki o wysokim stopniu specjalizacji: Aurora, RSA, APT1, Stuxnet

APT - charakterystyka

Advanced

Wykorzystywane przez osoby atakujące szeroką gamę technologii włamań i złośliwego oprogramowania, w tym tworzenie niestandardowego złośliwego oprogramowania, jeśli jest to wymagane.

Poszczególne komponenty niekoniecznie muszą być zaawansowane technicznie, ale są starannie dobierane, aby pasowały do wybranego celu.

APT - charakterystyka

Persistent

Zdecydowane stosowanie ataków przez dłuższy czas przeciwko wybranemu celowi, aby zmaksymalizować szanse powodzenia.

Różne ataki mogą być stosowane stopniowo, aż cel zostanie skompromitowany.

APT - charakterystyka

Threats

Zagrożenia dla wybranych celów w wyniku zorganizowanych, zdolnych i dobrze finansowanych napastników, którzy zamierzają złamać określone cele.

Aktywne zaangażowanie ludzi w proces znacznie podnosi poziom zagrożenia ze względu na narzędzia do automatycznych ataków, a także prawdopodobieństwo udanych ataków.

APT - charakterystyka

Cel: Spektrum celów - od kradzieży własności intelektualnej lub danych związanych z bezpieczeństwem i infrastrukturą do fizycznego zakłócenia infrastruktury.

Metodologia: Inżynieria społeczna, wiadomość e-mail typu spear-phishing, drive-by-download z wybranych zaatakowanych witryn, które mogą być odwiedzane przez personel docelowej organizacji.

Intencje: Aby zainfekować cel wyrafinowanym złośliwym oprogramowaniem z wieloma mechanizmami propagacji i ładunkami. Po uzyskaniu wstępnego dostępu do systemów w organizacji docelowej, do utrzymania i poszerzenia ich dostępu używa się dalszej gamy narzędzi atakujących

Malware - wirusy i robaki

Wirusy - komponenty

- Mechanizm infekcji
  - Środki, za pomocą których wirus rozprzestrzenia się lub namnaża
  - Nazywany również wektorem infekcyjnym
- Wyzwalacz (trigger)
  - Zdarzenie lub warunek przesądzające o uaktywnieniu lub dostarczeniu „ładunku” (ang. payload), niekiedy nazywanego bombą logiczną (ang. logic bomb).
- Ładunek (payload)
  - To, co wirus robi, pomijając rozprzestrzenianie się.

Wirusy

Wirus pozostaje bezczynny, do momentu, aż zostanie uaktywniony. Nie wszystkie wirusy posiadają tę fazę

Wirus zostaje uaktywniony, aby wykonać funkcję stanowiącą jego istotę. Podobnie jak w fazie uśpienia, faza wyzwalania może być spowodowana przez rozmaite zdarzenia systemowe, w tym wskutek wykonania przez kopię wirusa określonej liczby swoich kopii.

Wirus umieszcza swoją kopię w innych programach lub w specjalnych obszarach systemowych na dysku (polimorfizm).

Następuje wykonanie zamierzonej funkcji. Może to być funkcja nieszkodliwa, w rodzaju wyświetlenia komunikatu na ekranie, lub uszkadzająca, jak na przykład zniszczenie programów i plików z danymi.

Makrowirusy - wirusy makr

NISTIR 7298 definiuje makrowirusa jako:

„Wirus, który dołącza się do dokumentów i wykorzystuje funkcje programowania makr aplikacji dokumentu do wykonywania i rozprzestrzeniania się”

Wirusy makr infekują kod skryptowy używany do obsługi zawartości aktywnej w różnych typach dokumentów użytkownika

Makrowirusy - wirusy makr

Makrowirusy są groźne z kilku powodów

- Są niezależna od platformy
- Infekuj dokumenty, a nie wykonywalne fragmenty kodu
- Łatwo się rozprowadzają
- Ponieważ infekują one dokumenty użytkownika, a nie programy systemowe, tradycyjne mechanizmy kontroli dostępu do systemu plików mają ograniczone zastosowanie w zapobieganiu ich rozprzestrzenianiu, ponieważ użytkownicy powinni móc je modyfikować (pliki)
- Są znacznie łatwiejsze do napisania lub zmodyfikowania niż tradycyjne wirusy wykonywalne

Makrowirusy

```
macro Document Open
    disable Macro menu and some macro security features
    if called from a user document
        copy macro code into Normal template file
    else
        copy macro code into user document being opened
    end if
    if registry key "Melissa" not present
        if Outlook is email client
          for first 50 addresses in address book
               send email to that address
               with currently infected document attached
          end for
        end if
        create registry key "Melissa"
    end if
    if minute in hour equals day of month
        insert text into document being opened
    end if
end macro
```

Pseudokod wirusa Melissa (fragment)

Wirusy - klasyfikacja

Cel:

- Infektor sektora startowego - infekuje główny rekord rozruchowy lub rekord rozruchowy i rozprzestrzenia się, gdy system jest uruchamiany z dysku zawierającego wirusa
- Infektor plików - infekuje pliki, które system operacyjny lub powłoka uważa za wykonywalne
- Wirus makr - Infekuje pliki makrem lub kodem skryptów, który jest interpretowany przez aplikację
- Wirus wieloczęściowy - infekuje pliki na wiele sposobów

Wirusy - klasyfikacja

Strategia ukrywania:

- Zaszyfrowany wirus - część wirusa tworzy losowy klucz szyfrujący i szyfruje pozostałą część wirusa
- Wirus Stealth - forma wirusa specjalnie zaprojektowana do ukrywania się przed wykryciem przez oprogramowanie antywirusowe
- Wirus polimorficzny - wirus, który mutuje przy każdej infekcji
- Wirus metamorficzny - wirus, który mutuje i przepisuje się całkowicie w każdej iteracji i może zmieniać zachowanie oraz wygląd

Worms - robaki

- Program, który aktywnie wyszukuje więcej maszyn do zainfekowania, a każda zainfekowana maszyna służy jako automatyczna platforma startowa do ataków na inne maszyny
- Wykorzystuje luki w zabezpieczeniach oprogramowania w programach klienckich lub serwerowych
- Potrafi używać połączeń sieciowych do rozprzestrzeniania się z systemu do systemu
- Rozprzestrzenia się poprzez udostępnione media (dyski USB, dyski CD, DVD)
- Robaki pocztowe rozprzestrzeniają się w kodzie makr lub skryptu zawartym w załącznikach i przesyłanych plikach przez komunikatory internetowe
- Po aktywacji robak może się replikować i ponownie propagować
- Zwykle zawiera jakąś formę ładunku
- Pierwsza znana implementacja została wykonana w Xerox Palo Alto Labs na początku lat 80

Worms - propagacja

E-mail or IM	Robak wysyła swoją kopię e-mailem do innych systemów Robak się jako załącznik za pośrednictwem komunikatorów
File sharing	Tworzy własną kopię lub infekuje plik jako wirus na nośniku wymiennym
Remote execution capability	Robak wykonuje swoją kopię w innym systemie
Remote file access or transfer capability	Robak korzysta ze zdalnego dostępu do plików lub usługi przesyłania do kopiowania się z jednego systemu do drugiego
Remote login capability	Robak loguje się do zdalnego systemu jako użytkownik, a następnie używa poleceń do kopiowania się z jednego systemu do drugiego

Worms - propagacja

Skanowanie to pierwsza funkcja w fazie propagacji robaka sieciowego, który wyszukuje inne systemy do zainfekowania. Modele skanowania:

- Losowy
  - Każdy przejęty host sonduje losowe adresy w przestrzeni adresowej IP, używając innego ziarna
  - Powoduje to duży ruch w Internecie, który może powodować ogólne zakłócenia nawet przed rozpoczęciem rzeczywistego ataku
- Lista trafień
  - Osoba atakująca najpierw kompiluje długą listę potencjalnie podatnych maszyn
  - Po utworzeniu listy osoba atakująca zaczyna infekować maszyny znajdujące się na liście
  - Każda zainfekowana maszyna otrzymuje część listy do przeskanowania
  - Powoduje to bardzo krótki okres skanowania, co może utrudnić wykrycie, że ma miejsce infekcja

Worms - propagacja

- Topologiczny
  - Ta metoda wykorzystuje informacje zawarte na zainfekowanej maszynie ofiary, aby znaleźć więcej hostów do przeskanowania
- Lokalna podsieć
  - Jeśli host może zostać zainfekowany za zaporą ogniową, wówczas szuka celów we własnej sieci lokalnej
  - Host wykorzystuje strukturę adresów podsieci, aby znaleźć inne hosty, które w innym przypadku byłyby chronione przez zaporę

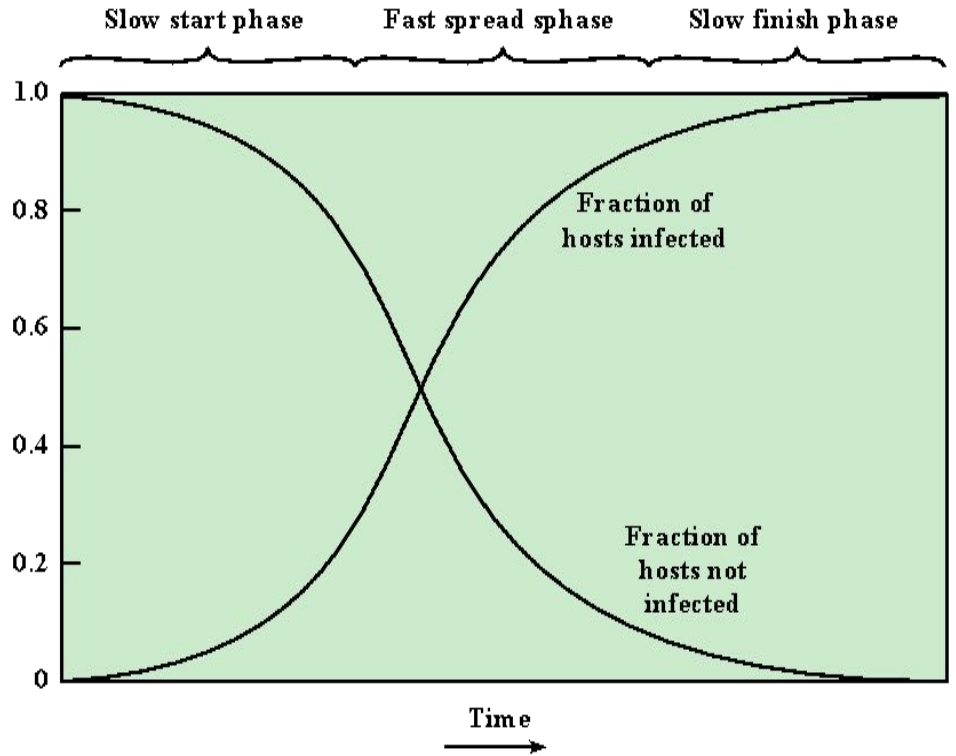
Robaki - model rozprzestrzeniania

Model propagacji jest podobny do wirusa biologicznego:

$$\frac{dI(t)}{dt} = \beta I(t)S(t)$$

$I(t)$	liczba zakażonych “osobników” w czasie t
$S(t)$	liczba podatnych “osobników” w czasie t
β	współczynnik rozmnażania

Worms - propagacja



Worms - historia

Melissaa	1998	E-mail worm. First to include virus, worm and Trojan in one package.
Code Red	July 2001	Exploited Microsoft IIS bug. Probes random IP addresses. Consumes significant Internet capacity when active.
Code Red II	August 2001	Also targeted Microsoft IIS. Installs a backdoor for access.
Nimda	September 2001	Had worm, virus and mobile code characteristics. Spread using e-mail, Windows shares, Web servers, Web clients, backdoors.
SQL Slammer	Early 2003	Exploited a buffer overflow vulnerability in SQL server compact and spread rapidly
Sobig.F	Late 2003	Exploited open proxy servers to turn infected machines into spam engines
Mydoom	2004	Mass-mailing e-mail worm. Installed a backdoor in infected machines
Warezov	2006	Creates executables in system directories. Sends itself as an e-mail attachment. Can disable security related products
Conficker (Downadup)	November 2008	Exploits a Windows buffer overflow vulnerability. Most widespread infection since SQL Slammer
Stuxnet	2010	Restricted rate of spread to reduce chance of detection. Targeted industrial control systems

Robak WannaCry

- Atak ransomware w maju 2017 r., który rozprzestrzeniał się niezwykle szybko w ciągu kilku godzin lub dni, infekując setki tysięcy systemów należących do organizacji publicznych i prywatnych w ponad 150 krajach.
- Rozprzestrzenia się jako robak, agresywnie skanując lokalne i losowe zdalne sieci, próbując wykorzystać lukę w usłudze udostępniania plików SMB w niezałatanych systemach Windows
- To szybkie rozprzestrzenianie się zostało spowolnione jedynie przez przypadkową aktywację domeny „wyłącznika awaryjnego” przez brytyjskiego badacza ds. Bezpieczeństwa
- Po zainstalowaniu na zainfekowanych systemach szyfruje również pliki, żądając zapłaty okupu za ich odzyskanie

Worms - stan technologiczny

Multi-platform

Polymorphic

Multi-exploit

Metamorphic

Ultrafast spreading

Kod mobilny

NIST SP 800-28 definiuje kod mobilny jako

„Programy, które można wysłać w niezmienionej postaci do heterogenicznego zbioru platform i wykonać z identyczną semantyką”

- Przesyłane z systemu zdalnego do systemu lokalnego, a następnie wykonywane w systemie lokalnym
- Często działa jako mechanizm wirusa, robaka lub konia trojańskiego
- Wykorzystuje luki w zabezpieczeniach do wykonywania własnych exploitów

Kod mobilny

Popularne pojazdy obejmują:

- Aplety Java
- ActiveX
- JavaScript
- VBScript

Najczęstsze sposoby wykorzystania kodu mobilnego do złośliwych operacji w systemie lokalnym to:

- Skrypty między witrynami
- Interaktywne i dynamiczne witryny internetowe
- Załączniki do wiadomości e-mail
- Pobieranie z niezaufanych witryn lub niezaufanego oprogramowania

Robaki mobilne

- Cabir - 2004 rok
- Lasco i CommWarrior - 2005 rok
- Komunikuje się za pośrednictwem połączeń bezprzewodowych Bluetooth lub wiadomości MMS.
- Może całkowicie wyłączyć telefon, usunąć dane z telefonu lub zmusić urządzenie do wysyłania kosztownych wiadomości
- **Najistotniejsze jednak jest to, że nielegalny kod zaimplementowany w urządzeniu mobilnym może służyć do zbierania informacji**
- **Obecnie najprostszym sposobem dostarczenia nielegalnego kodu jest użycie “trojana”**

Ataki “driven-by-downloads”

“Pobranie uboczne” - wykorzystuje luki w zabezpieczeniach przeglądarki i wtyczek, gdy użytkownik wyświetla stronę internetową kontrolowaną przez atakującego, Strona zawiera kod wykorzystujący błąd (w systemie użytkownika) do pobierania i instalowania złośliwego oprogramowania w systemie bez wiedzy i zgody użytkownika.

W większości przypadków złośliwe oprogramowanie nie rozprzestrzenia się aktywnie tak jak robak.

Ataki “Watering-Hole Attacks”

- Wariant ataku drive-by-download używany w wysoce ukierunkowanych atakach
- Atakujący bada swoje ofiary, aby zidentyfikować witryny, które prawdopodobnie odwiedzą, a następnie skanuje te witryny, aby zidentyfikować te z lukami.
- Następnie czekają, aż jedna z ich ofiar odwiedzi jedną z zaatakowanych stron
- Kod ataku może być nawet napisany tak, aby infekował tylko systemy należące do organizacji docelowej i nie podejmował żadnych działań wobec innych odwiedzających witrynę
- Takie działanie znacznie zwiększa prawdopodobieństwo, że włamanie na stronę pozostanie niewykryte

Socjotechnika

Spam

"Niechciana" poczta

Jedno z największych źródeł malware'u

Wykorzystywany do wykradania wszelkich danych

Konie trojańskie

Zawierają ukryty kod

Mogą być używane do pośredniego wykonywania czynności, których napastnik nie może wykonać bezpośrednio

Mobilne konie trojańskie

Nabywanie uprawnień root'a (jail-break)

Brak lub słaba kontrola jakości oprogramowania

Zapobieganie

- Idealnym (prawie niemożliwym do osiągnięcia) rozwiązaniem jest zapobieganie. Główne elementy zapobiegania to:
  - polityka bezpieczeństwa
  - świadomość
  - zmniejszanie podatności
  - łagodzenie zagrożeń - wykrywanie, identyfikacja, usunięcie

Programy antywirusowe

- Pierwsza generacja - analiza sygnatury (taki sam lub podobny wzorzec bitowy), dotyczy już znanego malware'u
- Druga generacja - skanery heurystyczne - poszukiwanie wzorców we fragmentach kodu (np. pętle szyfrujące)
- Trzecia generacja - programy rezydentne - analiza aktywności programów
- Czwarta generacja - złożone z rozmaitych technik antywirusowych stosowanych razem. Mamy tu składowe skanujące i pułapki aktywności

Sandbox

- Uruchamianie potencjalnie złośliwego kodu w emulowanej “piaskownicy” lub na maszynie wirtualnej
- Umożliwia wykonanie kodu w kontrolowanym środowisku, w którym jego zachowanie może być ściśle monitorowane bez zagrażania bezpieczeństwu rzeczywistego systemu
- Uruchamianie potencjalnie złośliwego oprogramowania w takich środowiskach umożliwia wykrycie złożonego, zaszyfrowanego, polimorficznego lub metamorficznego złośliwego oprogramowania
- Najtrudniejszym problemem projektowym związanym z analizą w “piaskownicy” jest określenie, jak długo należy uruchomić każdy potencjalnie szkodliwy kod

Analiza dynamiczna

- Host-Based Behavior-Blocking Software
- Integruje się z systemem operacyjnym komputera hosta i monitoruje zachowanie programu w czasie rzeczywistym pod kątem złośliwych działań
  - Blokuje potencjalnie złośliwe działania, zanim zdążą wpłynąć na system
  - Blokuje oprogramowanie w czasie rzeczywistym, dzięki czemu ma przewagę nad technikami wykrywania antywirusów, takimi jak odciski palców czy heurystyka

Analiza dynamiczna

Do monitorowanych zachowań mogą należeć:

- próby otwierania, oglądania, usuwania i (lub) modyfikowania plików
- próby formatowania dysków i wykonywania innych nieodtwarzalnych operacji dyskowych
- modyfikacje logiki plików wykonywalnych lub makrodefinicji
- zmiana krytycznych ustawień systemu, takich jak parametry rozruchowe
- oskryptowanie (ang. scripting) klientów poczty komunikatorów w celu wysyłania wykonywalnych treści
- inicjowanie komunikacji sieciowej

Skanowanie rozproszone

- Oprogramowanie antywirusowe zwykle dołączane do usług poczty e-mail i serwera proxy sieci Web działające na zaporze sieciowej organizacji i systemie IDS
- Może być również uwzględnione w komponencie analizy ruchu IDS
- Może obejmować środki zapobiegania włamaniom, blokujące przepływ podejrzanego ruchu
- Podejście ogranicza się do skanowania zawartości oprogramowania
- Analiza ruchu sieciowego - wykrywanie anomalii

Bezpieczeństwo systemów operacyjnych

Marek Miśkiewicz

wykład 6 i 7

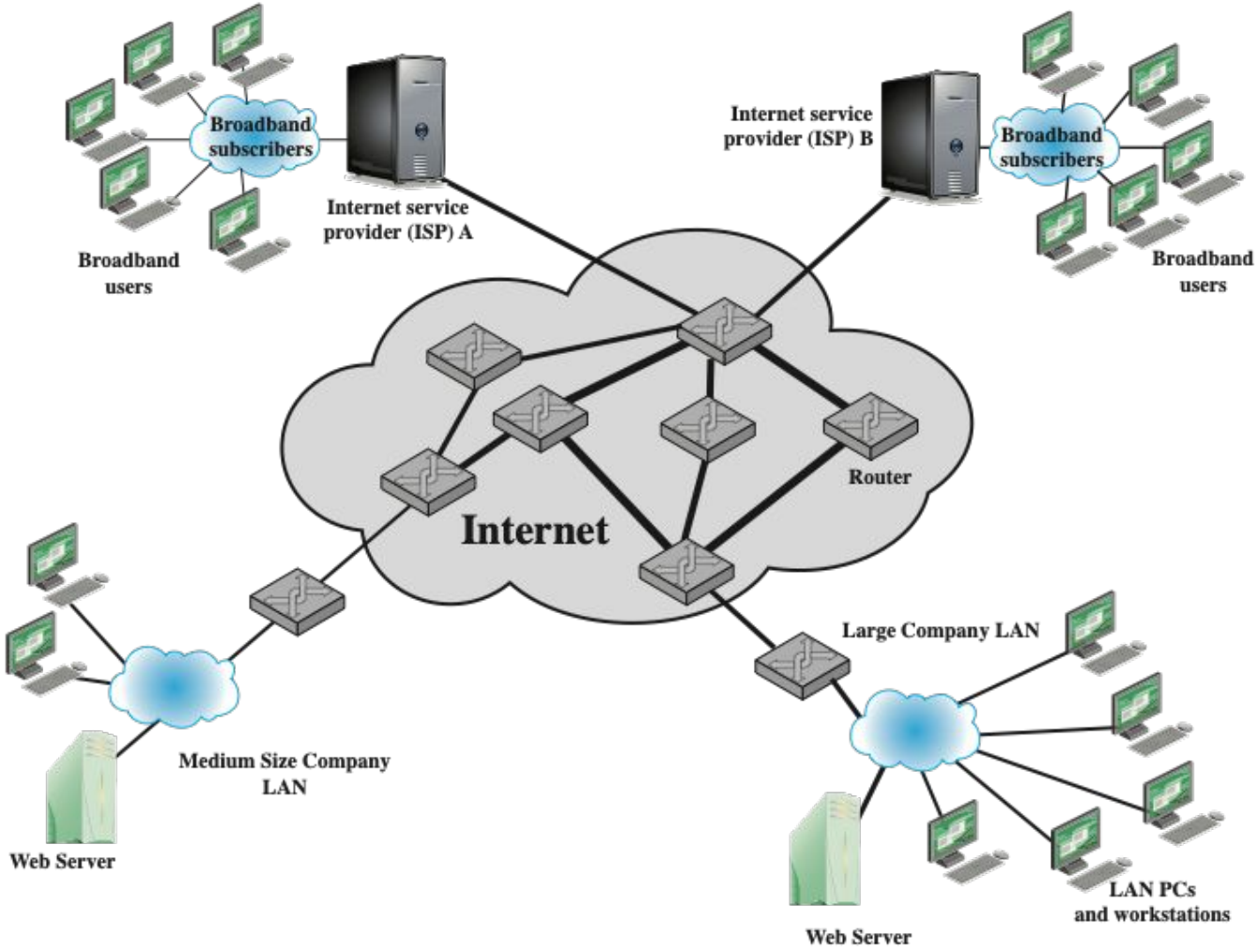
Ataki typu Denial-of-Service

DoS

NIST Computer Security Incident Handling Guide definiuje atak DoS jako:

„Działanie, które uniemożliwia lub utrudnia autoryzowane użycie sieci, systemów lub aplikacji poprzez wyczerpywanie zasobów, takich jak jednostki centralne (CPU), pamięć, przepustowość i miejsce na dysku”.

- Forma ataku na dostępność jakiejś usługi
- Kategorie zasobów, które mogą zostać zaatakowane, to:
  - łącze sieciowe
  - zasoby systemowe
  - zasoby aplikacji


Broadband subscribers
Broadband users
Internet service provider (ISP) A
Internet service provider (ISP) B
Broadband subscribers
Broadband users
Internet
Router
Medium Size Company LAN
Web Server
Large Company LAN
LAN PCs and workstations
Web Server

Klasyczne ataki DoS

Ping flood (pakiety ICMP)

- Celem tego ataku jest przeciążenie przepustowości połączenia sieciowego do organizacji docelowej
- Ruch musi być obsługiwany przez łącza o większej przepustowości na drodze do celu, pakiety są odrzucane wraz ze spadkiem pojemności
- Źródło ataku jest wyraźnie określone, chyba że zostanie użyty fałszywy adres
- Wydajność sieci jest zauważalnie ograniczona

Klasyczne ataki DoS

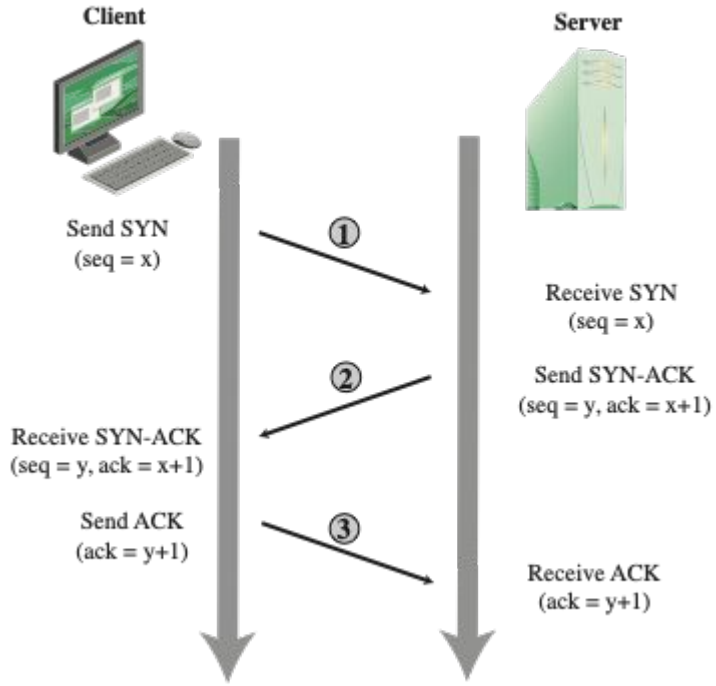
Adres spoofing

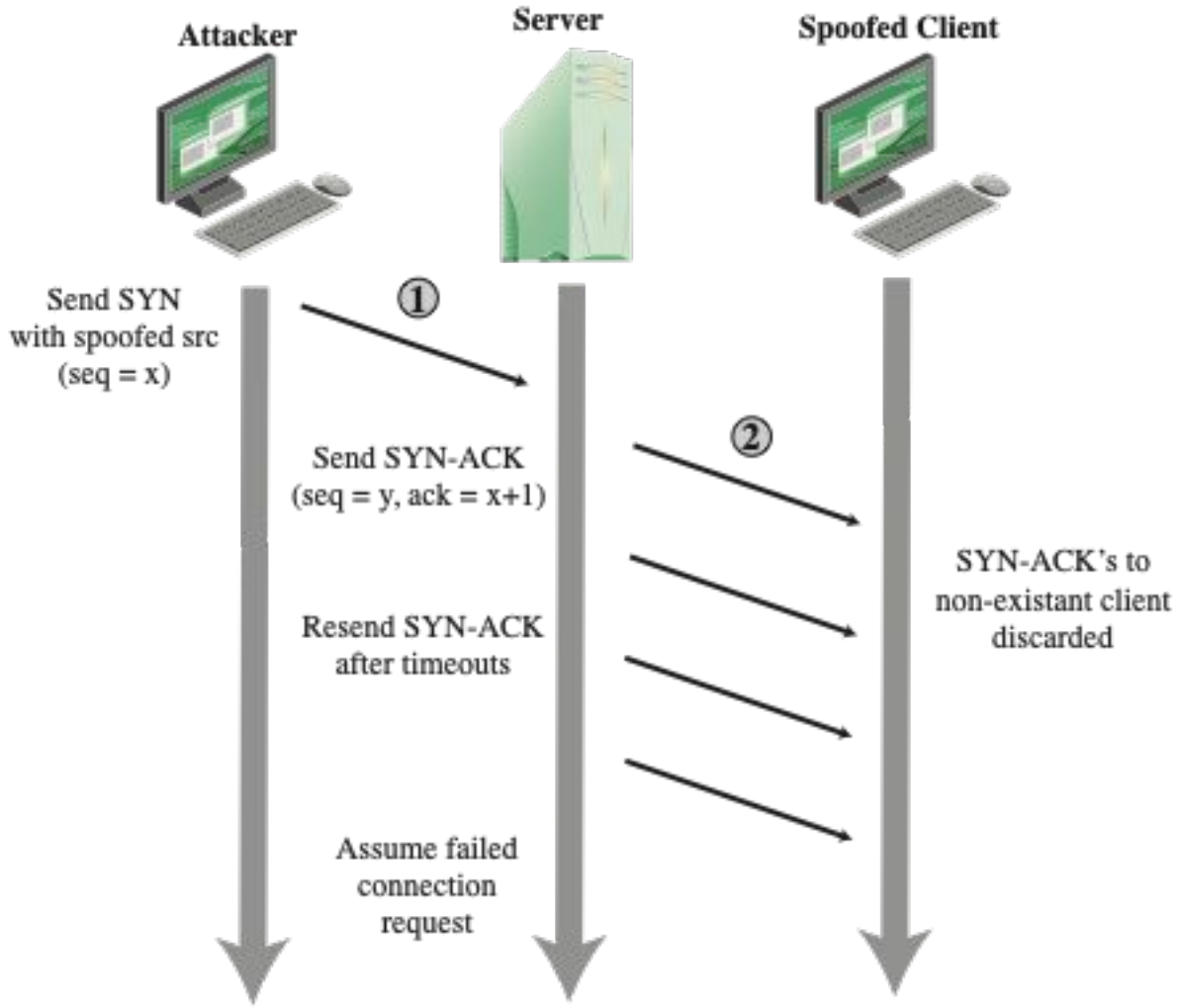
- Używa się fałszywych adresów źródłowych
  - Zwykle przez *raw socket interface* w systemach operacyjnych
  - W wyniku takiego zabiegu atakujące systemy są trudniejsze do zidentyfikowania
- Atakujący generuje duże ilości pakietów, których adresem docelowym jest system docelowy
- Zatory spowodowałyby podłączenie routera do ostatniego łącza o mniejszej przepustowości
- Wymaga od inżynierów sieciowych specjalnych zapytań o przepływ informacji ze swoich routerów
- Ruch wsteczny - *backscatter traffic*

Klasyczne ataki DoS

SYN spoofing

- Wykorzystuje specyfikę protokołu TCP - przeładowuje tablice nawiązywanych połączeń
- Opiera się na “three-way handshake” (protokół TCP jest niezawodny w przeciwieństwie do IP)
- SYN spoofing a SYN flooding

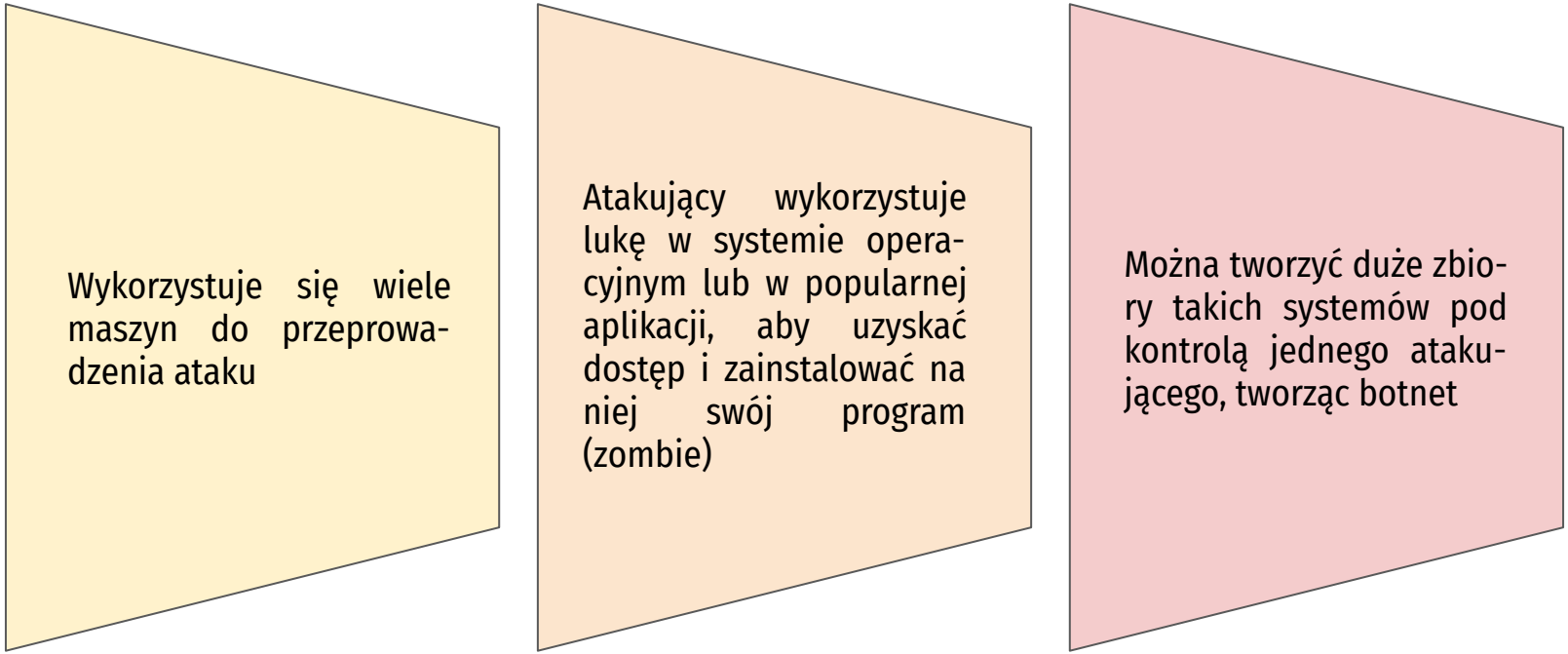


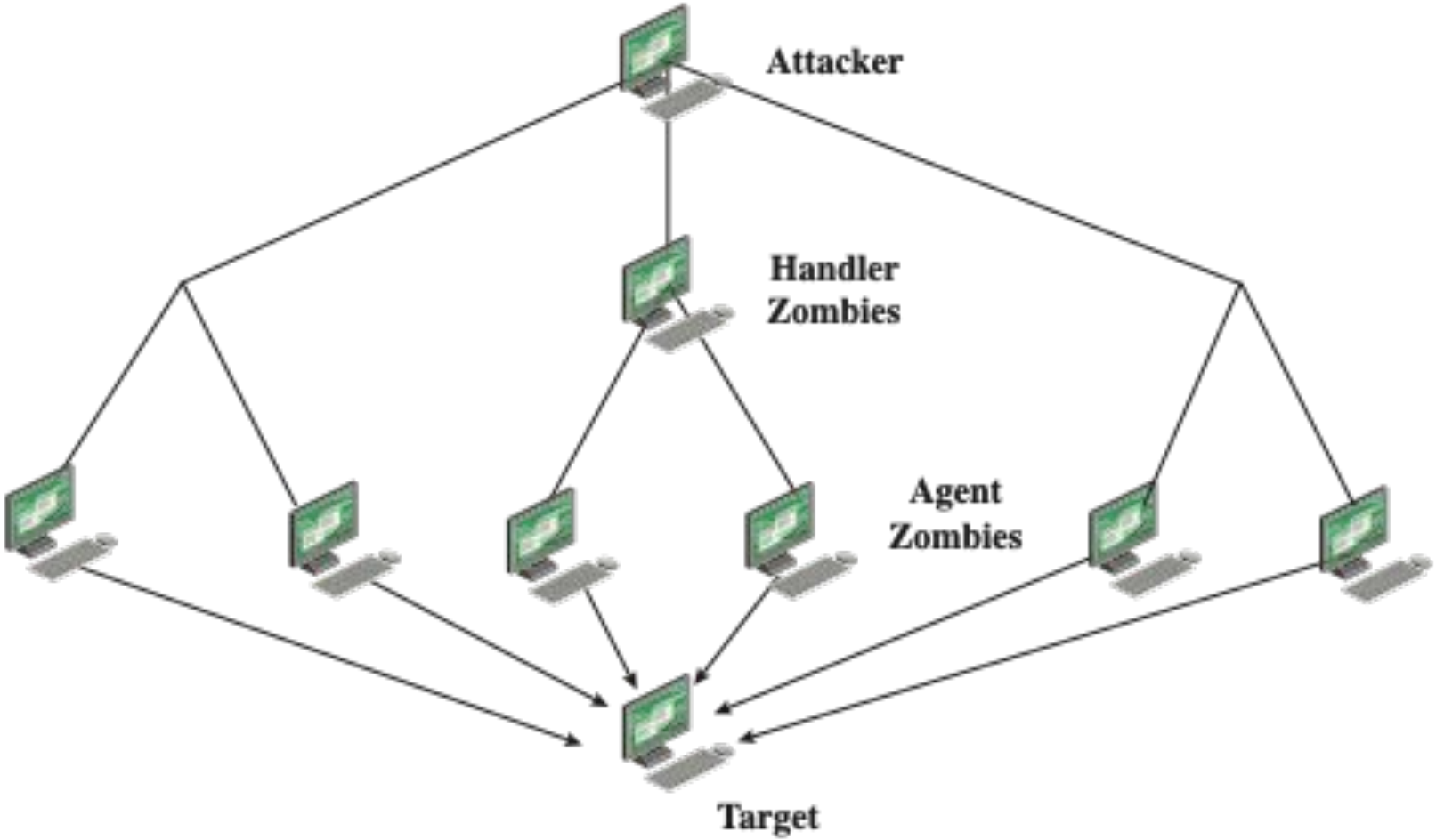

Attacker
Server
Spoofed Client
Send SYN
with spoofed src
(seq = x)
1
Send SYN-ACK
(seq = y, ack = x+1)
2
SYN-ACK's to
non-existant client
discarded
Resend SYN-ACK
after timeouts
Assume failed
connection
request

Ataki “zatapiające”

- Sklasyfikowane na podstawie używanego protokołu sieciowego
- Celem jest przeciążenie przepustowości sieci na jakimś łączu do serwera
- Można zastosować praktycznie każdy typ pakietu sieciowego
- ICMP flood:
  - Ping flood przy użyciu pakietów żądania echa ICMP
  - Tradycyjnie administratorzy sieci zezwalają na takie pakiety w swoich sieciach, ponieważ ping jest przydatnym narzędziem diagnostycznym sieci
- UDP flood:
  - Używa pakietów UDP skierowanych do jakiegoś numeru portu w systemie docelowym
- TCP SYN flood:
  - Wysyła pakiety TCP do systemu docelowego
  - Celem ataku jest całkowita objętość pakietów, a nie kod systemowy

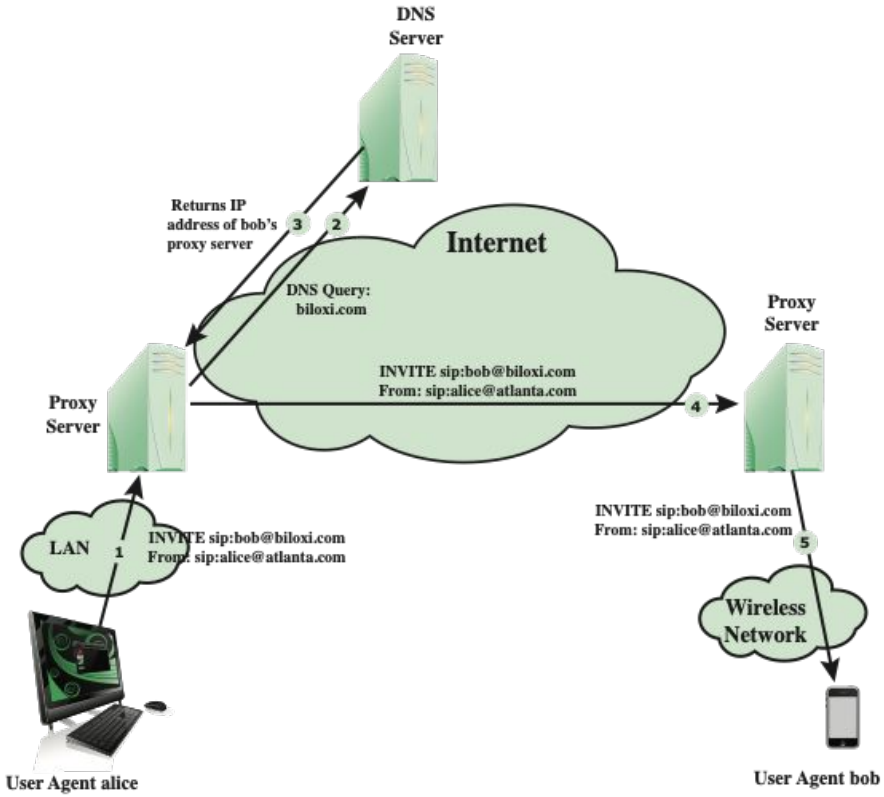
Ataki DDoS - Distributed Denial of Service




Attacker
Handler
Zombies
Agent
Zombies
Target

SIP flood

- SIP - Session Initiation Protocol - protokół VoIP, tekstowy podobny do HTTP
- pojedynczy INVITE zużywa znaczne ilości zasobów
- atakujący może zalać pośrednika SIP dużą ilością zamówień INVITE z fałszywymi adresami IP lub wykonać atak DDoS za pomocą botnetu generującego wiele zamówień INVITE
- atak obciąża serwery pośredniczące w SIP dwojako:
  - zasoby wyczerpują się podczas przetwarzania zamówień INVITE
  - zużywana jest pojemność ich sieci



Ataki bazujące na protokole HTTP

HTTP flood:

- Atak, który bombarduje serwery WWW żądaniami HTTP
- Zużywa znaczne zasoby
- Spidering - boty rozpoczynające wysyłanie żądań od podanego linku HTTP i podążające rekurencyjnie za wszystkimi linkami w podanej witrynie internetowej

Ataki bazujące na protokole HTTP

Slowloris:

- wykorzystuje popularną technikę polegającą na zastosowaniu wielu wątków do obsługi wielu zamówień w tej samej aplikacji serwera
- próbuje “zmonopolizować” sesje, wysyłając żądania HTTP, które nigdy się nie kończą - brak “pustego wiersza” kończącego zamówienie
- ostatecznie prowadzi to do zużycia przepustowości połączenia serwera internetowego
- technika wykorzystuje legalny ruch HTTP
- istniejące rozwiązania do wykrywania włamań i zapobiegania im, które opierają się na sygnaturach do wykrywania ataków, generalnie nie rozpoznają Slowloris

Ataki bazujące na protokole HTTP

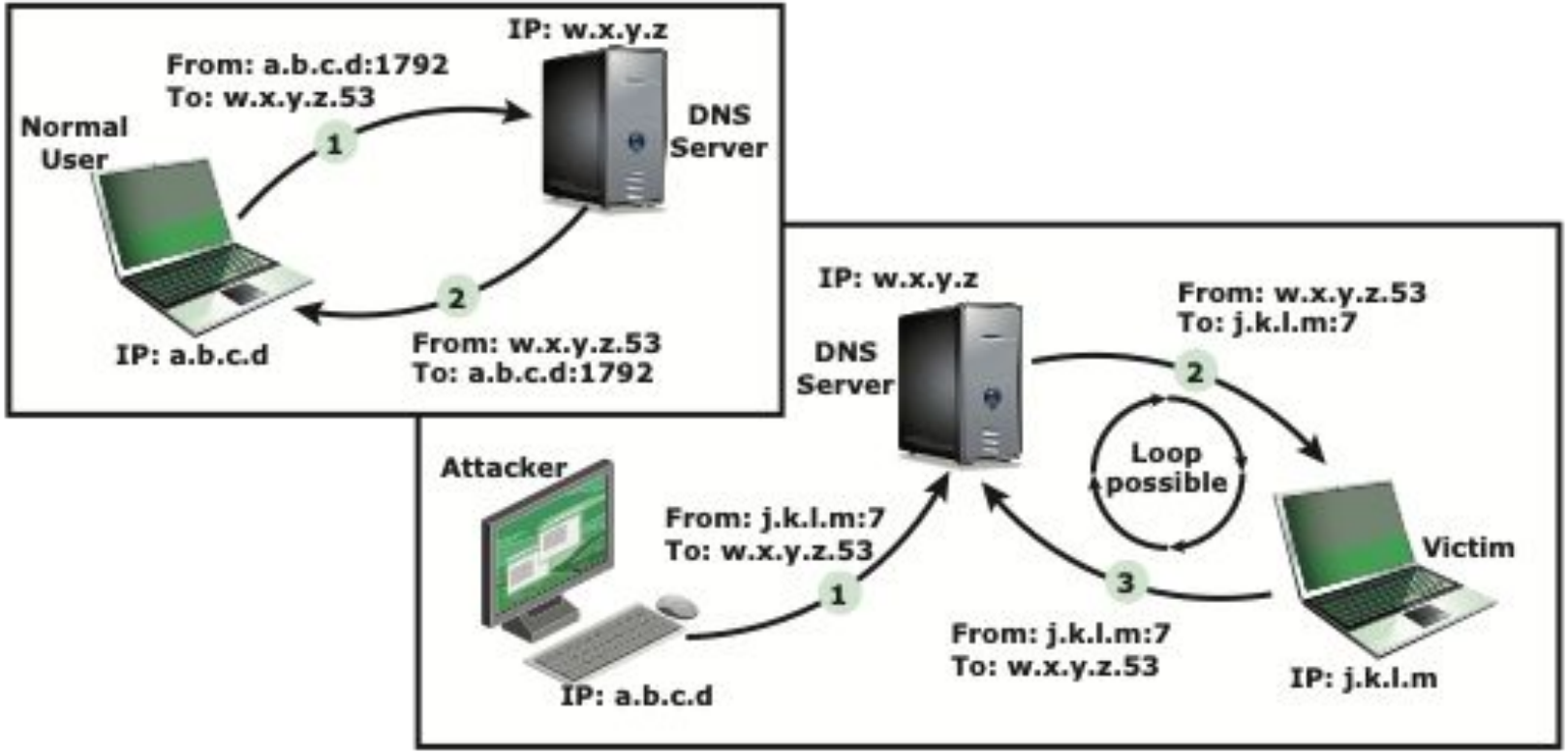
Slowloris:

- metody zapobiegania:
  - ograniczanie tempa zamówień nadchodzących (przyjmowanych) z konkretnego hosta
  - zmienianie czasu oczekiwania na (aktywne) połączenia w funkcji liczby połączeń i opóźnianie wiązań - oczekiwanie z wysłaniem zamówienia dopóki klient nie wyśle poprawnych schematów ze znakami końca linii

Ataki “z odbicia” - reflection attacks

- Atakujący wysyła pakiety do znanej usługi pośrednika ze sfałszowanym adresem źródłowym rzeczywistego systemu docelowego
- Gdy pośrednik odpowiada, odpowiedź jest wysyłana do celu
- Celem jest wygenerowanie wystarczającej ilości pakietów, aby zalać łącze do systemu docelowego bez powiadamiania pośrednika
- Podstawową obroną przed tymi atakami jest blokowanie pakietów ze sfałszowanych źródeł

Ataki “z odbicia” - reflection attacks



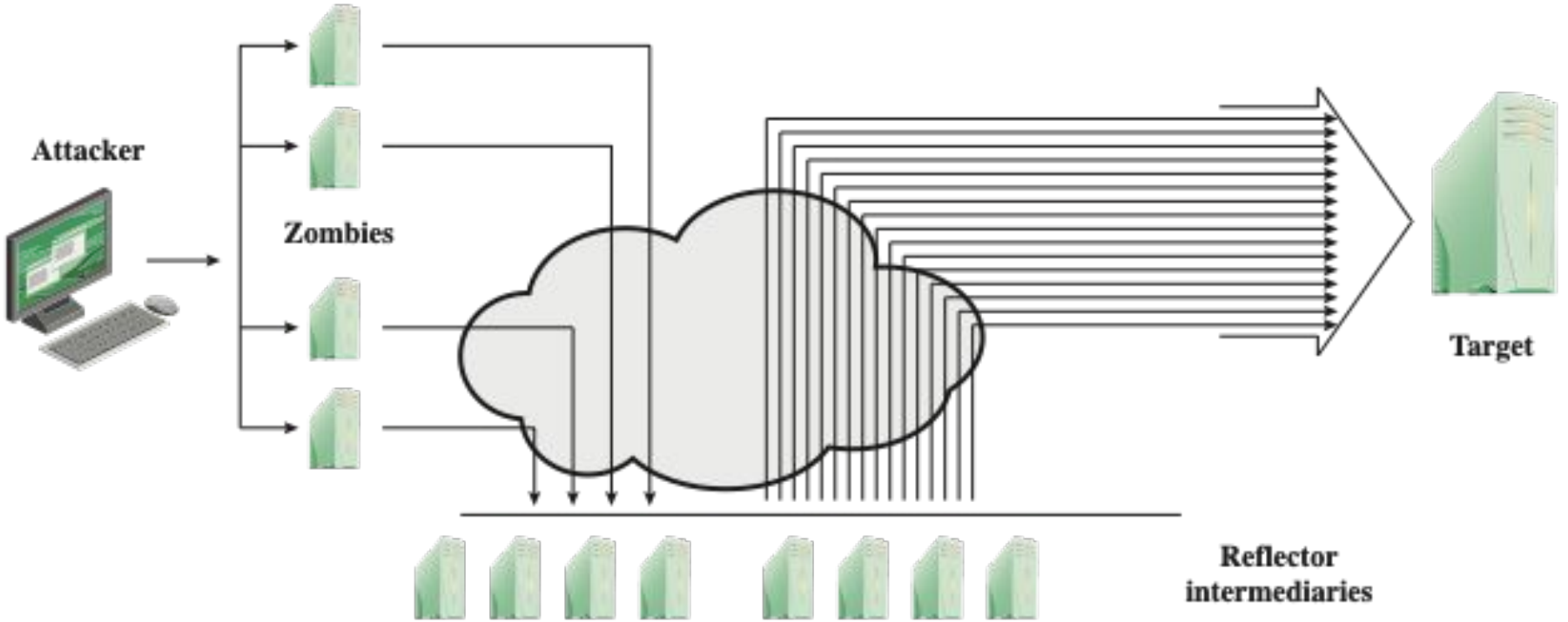
Ataki “ze wzmocnieniem”- amplification attacks

- są odmianą *reflection attacks*
- najczęściej używa się pakietów skierowanych do legalnego serwera DNS jako systemu pośredniczącego z fałszywymi adresami nadania (ofiara)
- generowanie wielu pakietów z odpowiedzią - można to osiągnąć przez skierowanie pierwotnego zamówienia pod adres rozgłaszania w jakiejś sieci
- potencjalnie wszystkie komputery w tej sieci mogą odpowiedzieć na to zamówienie
- wykorzystuje się protokoły ICMP i UDP (echo)
- protokół i usługi TCP nie nadają się do tego typu ataków

Ataki “ze wzmocnieniem”- oparte na DNS

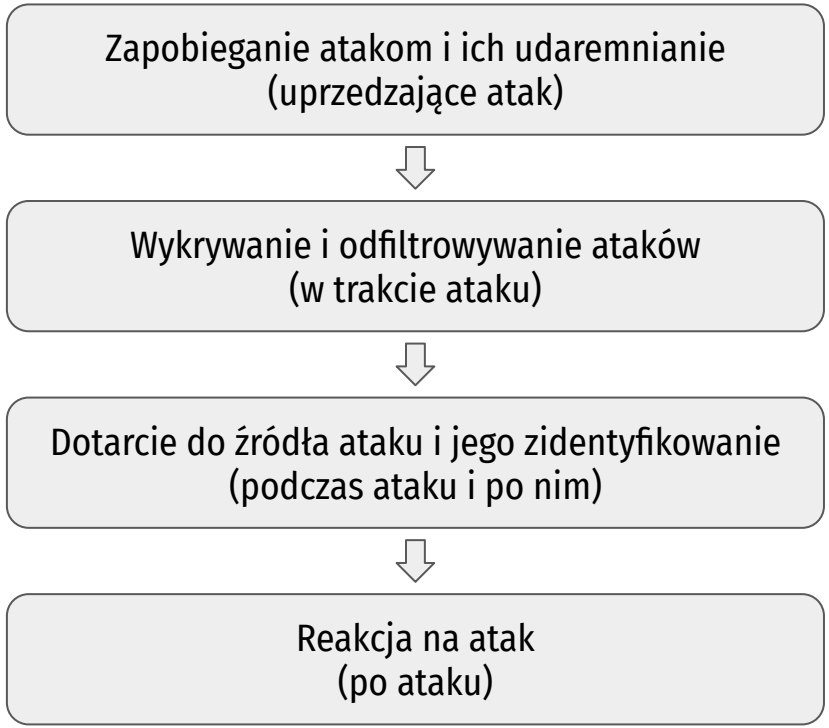
- odmiana ataku *reflection DNS* wykorzystująca cechy protokołu
  - atakujący tworzy ciąg zamówień DNS zawierających fałszywy adres źródłowy, będący adresem atakowanego systemu
  - zapytania są kierowane do pewnej liczby wybranych serwerów DNS
  - serwery odpowiadają, wysyłając odpowiedzi do fałszywego źródła, które uznają za poprawny system zamawiający co powoduje, że cel jest wtedy zalewany ich odpowiedziami
- istnieje wariant tego ataku, do przeprowadzenia którego wykorzystywany jest serwer DNS akceptuj zapytania rekurencyjne, ponieważ wzmocnione pakiety DNS są odpowiedziami na rekursywne zapytania DNS

Ataki “ze wzmocnieniem”- amplification attacks



Ataki DoS i DDoS - obrona

- Atakom tym nie można całkowicie zapobiec
- Duże natężenie ruchu może być uzasadnione
  - duża czasowa popularność określonej witryny
  - wysoka czasowa aktywność w bardzo popularnej witrynie
  - zjawiska opisywane jako slashdotted, flash crow lub flash event



Ataki DDoS - prewencja

- Blokowanie fałszywych adresów źródłowych na routerach jak najbliżej źródła
- Filtry mogą być używane, aby zapewnić, że ścieżka powrotna do żądanego adresu źródłowego jest tą, z której korzysta bieżący pakiet
- Filtry muszą być stosowane do ruchu, zanim opuści on sieć dostawcy usług internetowych lub w punkcie wejścia do jego sieci
- Użycie zmodyfikowanego kodu obsługi połączenia TCP - szyfrowanie kryptograficzne krytycznych informacji w pliku cookie, który jest wysyłany jako początkowy numer sekwencyjny serwera. Legalny klient odpowiada pakietem ACK zawierającym plik cookie ze zwiększonym numerem sekwencji
- Usuwanie wpisów dotyczących niekompletnego połączenia z tabeli połączeń TCP w przypadku przepełnienia

Ataki DDoS - prewencja

- Blokuj rozgłaszania kierowane przez IP
- Blokuj podejrzane usługi i kombinacje
- Zarządzaj atakami na aplikacje wykorzystując (captcha), aby rozróżniać uzasadnione żądania ludzi
- Dobre ogólne praktyki bezpieczeństwa systemu
- Używaj serwerów lustrzanych i replikowanych, gdy wymagana jest wysoka wydajność i niezawodność

Ataki DoS i DDoS - odpowiedź

- Identyfikacja rodzaj ataku
  - przechwytuj i analizuj pakiety
  - zaprojektuj filtry, aby blokować ruch związany z atakami
  - zidentyfikuj i popraw błąd systemu / aplikacji
- Zlecenia ISP śledzenia przesyłanie pakietów (analiza odwrotnej drogi)
  - Może być trudne i czasochłonne
  - Konieczne przy planowaniu działań prawnych
- Wdrożenie planu awaryjnego
  - Przełącz się na alternatywne serwery kopii zapasowych
  - Uruchom nowe serwery w nowej witrynie z nowymi adresami
- Aktualizacja planu reagowania na incydenty
  - Przeanalizuj atak i odpowiedź na przyszłe działania

Detekcja włamań

Klasyfikacja intruzów - cyberprzestępcy

- Osoby indywidualne albo członkowie zorganizowanych grup przestępczych, których celem są korzyści finansowe
- Aktywność:
  - kradzież tożsamości
  - kradzież poświadczeń finansowych
  - szpiegostwo korporacyjne
  - kradzież danych lub szantażowanie danymi
- młodzi hakerzy, często z Europy Wschodniej, Rosji lub południowo-wschodniej Azji, robiący interesy w Sieci
- bardzo duże i wzrastające koszty wynikające z cyberprzestępczej aktywności, są powodem do podejmowania kroków w celu minimalizowana tego zagrożenia

Klasyfikacja intruzów - aktywiści

- Osoby, które zwykle pracują jako osoby zatrudnione wewnątrz organizacji, czy też członkowie większej grupy napastników z zewnątrz, którzy są zmotywowani ze względów społecznych lub politycznych
- Znani również jako haktywiści - poziom umiejętności jest często dość niski
- Celem ich ataków jest często promowanie i nagłaśnianie ich sprawy, zazwyczaj poprzez:
  - Zniszczenie witryny
  - Ataki typu „odmowa usługi”
  - Kradzież i dystrybucja danych, która prowadzi do negatywnego rozgłosu lub narażania celów

Klasyfikacja intruzów - organizacje sponsorowane

- Grupy hakerów sponsorowanych przez rządy w celu prowadzenia działań szpiegowskich lub sabotażowych
- Znane również jako zaawansowane trwałe zagrożenia (APT) ze względu na ukryty charakter i wytrwałość przez dłuższy czas związane z wszelkimi atakami z tej klasy
- Ujawniane co pewien czas informacje wskazują na rozległy charakter i zakres takiej działalności prowadzonej przez dużą grupę krajów

Klasyfikacja intruzów - inni

- Hakerzy z motywacjami innymi niż wymienione wcześniej
- “Klasyczni” hakerów lub crackerzy, których motywuje wyzwanie techniczne lub szacunek i reputacja w grupie rówieśniczej
- Wiele osób w tej kategorii odpowiedzialnych jest za wykrywanie nowych kategorii luk i można uznać ich za członków tej klasy
- Biorąc pod uwagę szeroką dostępność zestawów narzędzi do ataków, istnieje grupa „hakerów hobbystów”, którzy używają tych zestawów do badania systemu i bezpieczeństwa sieci

Klasyfikacja intruzów - poziom I

- Hakerzy o minimalnych umiejętnościach technicznych, którzy głównie używają istniejących zestawów narzędzi do ataku
- Prawdopodobnie stanowią największą liczbę napastników, w tym wielu przestępców i aktywistów
- Biorąc pod uwagę wykorzystanie przez nich istniejących znanych narzędzi, najłatwiej jest się przed nimi obronić
- Znany również jako „script-kiddies” ze względu na wykorzystanie istniejących skryptów (narzędzi)

Klasyfikacja intruzów - poziom II

- Hakerzy posiadający wystarczające umiejętności techniczne, aby modyfikować i rozszerzać zestawy narzędzi do ataków, aby wykorzystywać nowo odkryte lub “zakupione” luki w zabezpieczeniach
- Mogą być w stanie zlokalizować nowe luki w zabezpieczeniach do wykorzystania, podobne do niektórych już znanych
- Hakerzy z takimi umiejętnościami prawdopodobnie znajdują się we wszystkich klasach intruzów
- Są w stanie dostosować narzędzia używane przez innych

Klasyfikacja intruzów - poziom III

- Hakerzy o wysokich umiejętnościach technicznych, zdolni do wykrywania zupełnie nowych kategorii luk w zabezpieczeniach (APT)
- Piszą nowe zestawy narzędzi do ataku
- Niektórzy są zatrudniani przez organizacje sponsorowane przez państwo
- Obrona przed tymi atakami jest najtrudniejsza

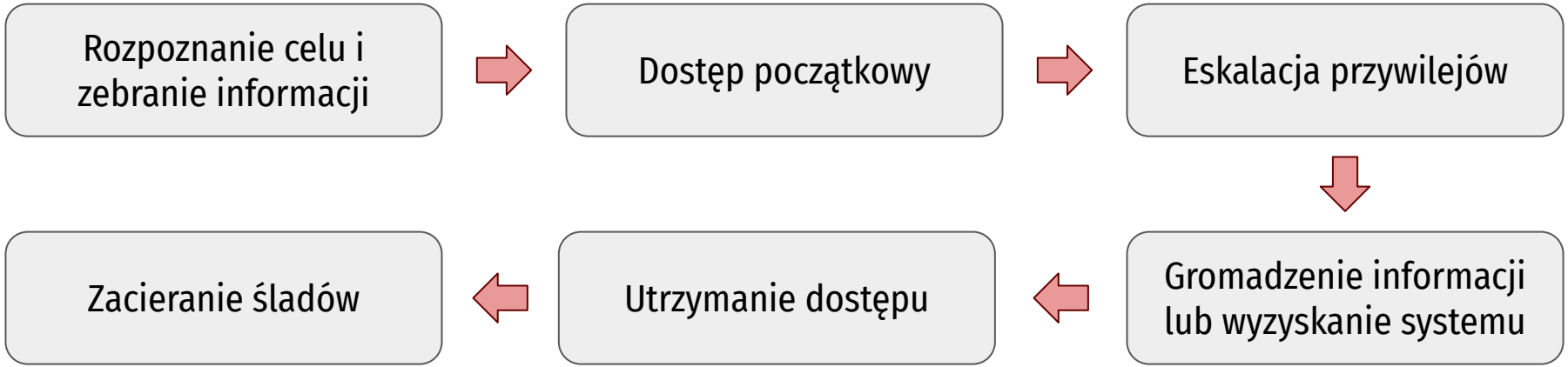
Przykłady włamań i naruszeń

- zdalne przejęcie funkcji administratora serwera poczty elektronicznej
- zniszczenie serwera Sieci
- odgadnięcie i złamanie haseł
- skopiowanie bazy danych zawierającej numery kart kredytowych
- oglądanie bez upoważnienia poufnych danych, w tym list płac i informacji medycznych
- uruchomienie podsłuchiwacza pakietów na stacji roboczej w celu przechwycenia nazw użytkowników i haseł

Przykłady włamań i naruszeń

- wykorzystanie błędu w pozwoleniach na anonimowym serwerze FTP do rozpowszechniania pirackiego oprogramowania i plików
- zatelefonowanie do niezabezpieczonego modemu i uzyskanie dostępu do wewnętrznej sieci
- upozowanie się na kierownika, zadzwonienie do działu pomocy, ustalenie nowego hasła do poczty kierownika i przyswojenie nowego hasła;
- użycie bez pozwolenia pozostawionej bez opieki, zalogowanej stacji roboczej.

Ogólny schemat



Wykrywanie włamań - pojęcia

Naruszenie bezpieczeństwa (włamanie do systemu zabezpieczeń, ang. security intrusion) - bezprawny akt obejścia mechanizmów bezpieczeństwa systemu.

Wykrywanie włamań (wykrywanie wtargnięć, ang. intrusion detection) - realizowana sprzętowo lub programowo funkcja gromadzenia i analizowania informacji z różnych obszarów w obrębie komputera lub sieci, mająca na celu zidentyfikowanie ewentualnych naruszeń bezpieczeństwa.

IDS - Intrusion Detection System - system wykrywania włamań

IPS - Intrusion Prevention System - systemy zapobiegania włamaniom

IDS - komponenty logiczne

Czujniki - odpowiadają za gromadzenie danych. Wejściem czujnika może być dowolna część systemu, która może zawierać dowody włamania. Do rodzajów danych wejściowych czujników należą pakiety sieciowe, pliki dzienników i ślady wywołań systemowych. Czujniki gromadzą i przekazują te informacje analizatorowi.

Analizatory - otrzymują dane od jednego lub więcej czujników lub od innych analizatorów. Analizator odpowiada za ustalenie, czy doszło do włamania. Na wyjściu tego komponentu jest wskazanie (sugestia), że mogło dojść do włamania.

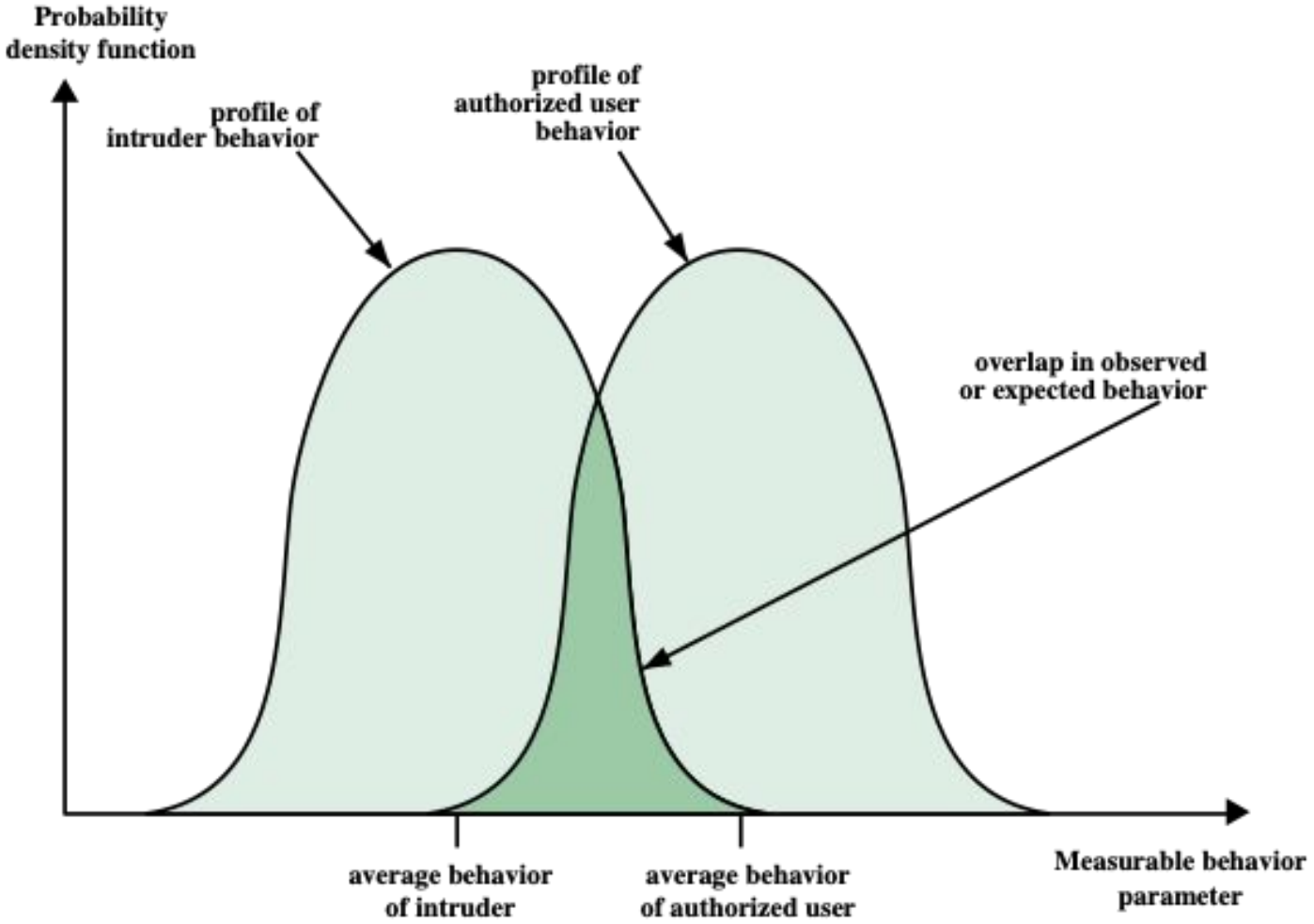
Interfejs użytkownika - umożliwia użytkownikowi obejrzenie wyników z systemu lub pokierowanie zachowaniem systemu.

IDS’y - klasyfikacja

- **IDS-y hostowe (zadomowione, HIDS)** - monitorują charakterystyki pojedynczego komputera sieciowego (na przykład identyfikatory procesów) i występujące w nim zdarzenia (takie jak wykonywane przez procesy wywołania systemowe), aby uwidaczniać podejrzane działania.
- **IDS-y sieciowe (usieciowione, NIDS)** - monitorują ruch w poszczególnych odcinkach sieci lub w jej urządzeniach oraz analizują sieć, trans- port i protokoły aplikacji w celu identyfikowania podejrzanych działań.
- **IDS-y rozproszone lub hybrydowe** - łączą informacje z wielu czujników, często zarówno rozlokowanych w komputerach, jak i w sieci, gromadząc je w centralnym analizatorze, który potrafi lepiej identyfikować działania towarzyszące włamaniom i reagować na nie.

IDS’y

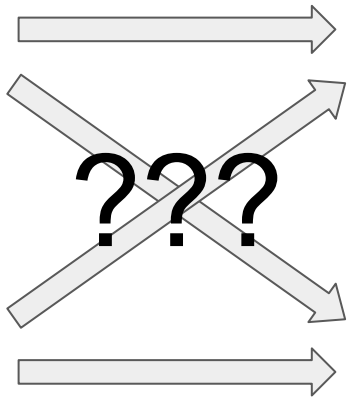
Wykrywanie włamań bazuje się na założeniu, że zachowanie napastnika różni się w jakiś sposób od działania legalnego użytkownika, w szczególności, w sposób dający się określić ilościowo. Nie możemy oczekiwać ostrej, wyraźnej różnicy między atakiem a normalnym użytkowaniem zasobów przez upoważnionego użytkownika. Musimy przyjąć, że zjawiska te będą “rozmyte” i będą na siebie zachodziły.


Probability
density function
profile of
intruder behavior
profile of
authorized user
behavior
overlap in observed
or expected behavior
average behavior
of intruder
average behavior
of authorized user
Measurable behavior
parameter

IDS’y

Mała ilość alarmów

Duża ilość alarmów



Wysoka skuteczność

Wysokie bezpieczeństwo

IDS’y - wymagania

Wymagane cechy IDS’ów:

- Ciągłe działanie, wymagające minimalnego nadzoru.
- Tolerowanie awarii w tym sensie, że oprogramowanie to potrafi się reaktywować po zatrzymaniu systemu i jego ponownym uruchomieniu.
- Odporność na działania ukierunkowane na IDS. IDS musi sam siebie monitorować i wykrywać, czy nie został zmodyfikowany przez atakującego.
- Wprowadzanie minimalnego obciążenia do systemu.
- Możliwość skonfigurowania zgodnie z zasadami bezpieczeństwa analizowanego środowiska.

IDS’y - wymagania

Wymagane cechy IDS’ów:

- Zdolność do adaptacji w miarę wprowadzania zmian w systemie i zmian w zachowaniach użytkowników.
- Zdolność do skalowalności.
- Łagodna degradacja usług — jeśli jakieś usługi składowe IDS-u przestają z jakiegoś powodu działać, oddziałuje to na pozostałe w jak najmniejszym stopniu.
- Umożliwianie dynamicznej rekonfiguracji, bez potrzeby restartowania IDS-u.

IDS’y - wykrywanie - podejście analityczne

- **Detekcja oparta na anomaliach:**
  - Obejmuje gromadzenie danych dotyczących zachowania legalnych użytkowników przez określony czas
  - Aktualnie obserwowane zachowanie jest analizowane w celu ustalenia, czy jest to zachowanie legalnego użytkownika, czy intruza
- **Detekcja oparta na sygnaturach (heurystykach):**
  - Używa zestawu znanych złośliwych wzorców danych lub reguł ataku, które są porównywane z bieżącym zachowaniem
  - Znane również jako wykrywanie nadużyć
  - Potrafi zidentyfikować tylko znane ataki, dla których ma wzorce lub reguły

IDS’y - detekcja oparta na anomaliach

Statystyczna - analiza obserwowanego zachowania z użyciem modeli jedno- lub wieloczynnikowych lub modeli szeregów czasowych obserwowanych metryk.

Oparta na wiedzy - metody, w których są używane systemy eksperckie klasyfikujące obserwowane zachowanie według zbioru reguł modelujących legalne zachowanie.

Uczenie maszynowe - metody automatycznego określania odpowiedniego modelu klasyfikacji na podstawie danych treningowych, z użyciem technik eksploracji danych.

IDS’y - detekcja oparta na sygnaturach

Sygnatury

- dopasowanie dużego zbioru znanych wzorców szkodliwych danych do danych przechowywanych w systemie lub przesyłanych przez sieć
- sygnatury muszą być wystarczająco duże, aby zminimalizować wskaźnik fałszywych alarmów, jednocześnie wykrywając wystarczająco dużą część złośliwych danych
- metoda szeroko stosowana w produktach antywirusowych, serwerach proxy do skanowania ruchu sieciowego oraz w NIDS

IDS’y - Identyfikacja heurystyczna oparta na regułach

Reguły

- obejmuje stosowanie reguł identyfikacji znanych podatności lub penetracji, które wykorzystywałyby znane słabości
- można także zdefiniować reguły, które identyfikują podejrzane zachowanie, nawet jeśli jest ono w granicach ustalonych wzorców użytkowania

HIDS - Host based IDS

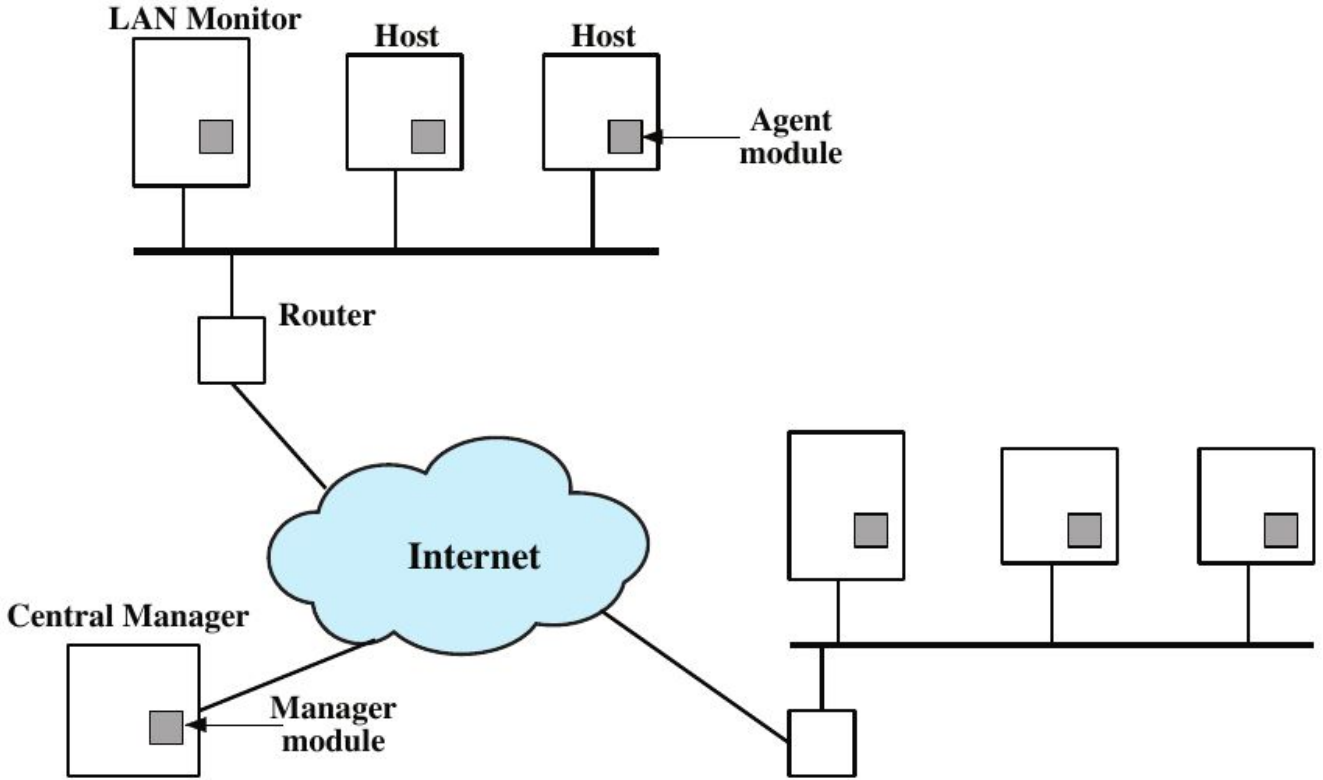
- Dodaje wyspecjalizowaną warstwę oprogramowania zabezpieczającego do wrażliwych lub wrażliwych systemów
- Może korzystać z anomalii lub sygnatur i metod heurystycznych
- Monitoruje aktywność w celu wykrycia podejrzanego zachowania
  - głównym celem jest wykrywanie włamań, rejestrowanie podejrzanych zdarzeń i wysyłanie alertów
  - potrafi wykryć zarówno włamania zewnętrzne, jak i wewnętrzne

HIDS - źródła i czujniki danych

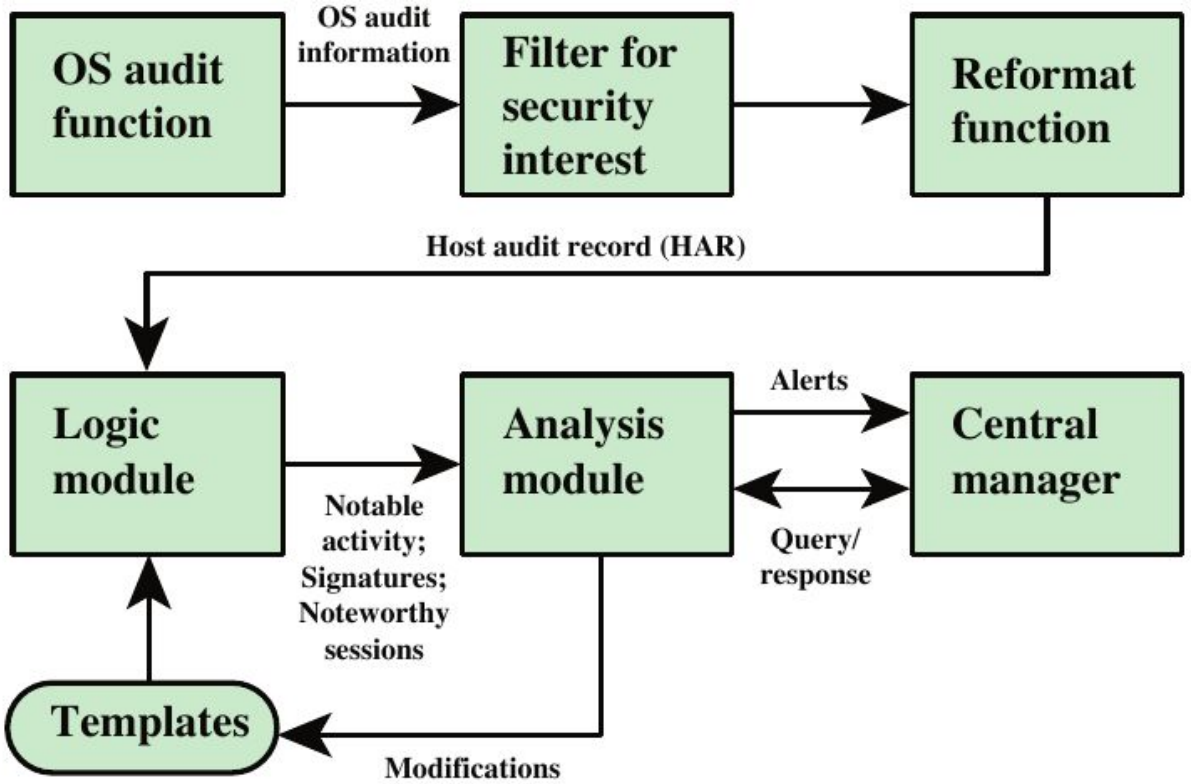
Do typowych źródeł danych należą:

- **ślady wywołań systemowych** - zapisy ciągów wywołań systemowych wykonywanych przez procesy w systemie są powszechnie uznawane za wartościowe źródło danych HIDS-u (Linux - ok, Windows - problematyczne)
- **rekordy audytu (plik dziennika)** - zaleta: nie trzeba korzystać z żadnego dodatkowego oprogramowania do ich gromadzenia, wada: rekordy audytu mogą nie zawierać potrzebnych informacji; intruzi mogą próbować manipulować tymi zapisami, aby ukryć swoje ataki.
- **sumy kontrolne nienaruszalności plików** - okresowe skanowanie krytycznych plików pod kątem rozbieżności z pożądanym wzorem przez porównywanie bieżących kryptograficznych sum kontrolnych tych plików z zapisem znanych, dobrych wartości

HIDS - rozproszony



HIDS - architektura agenta



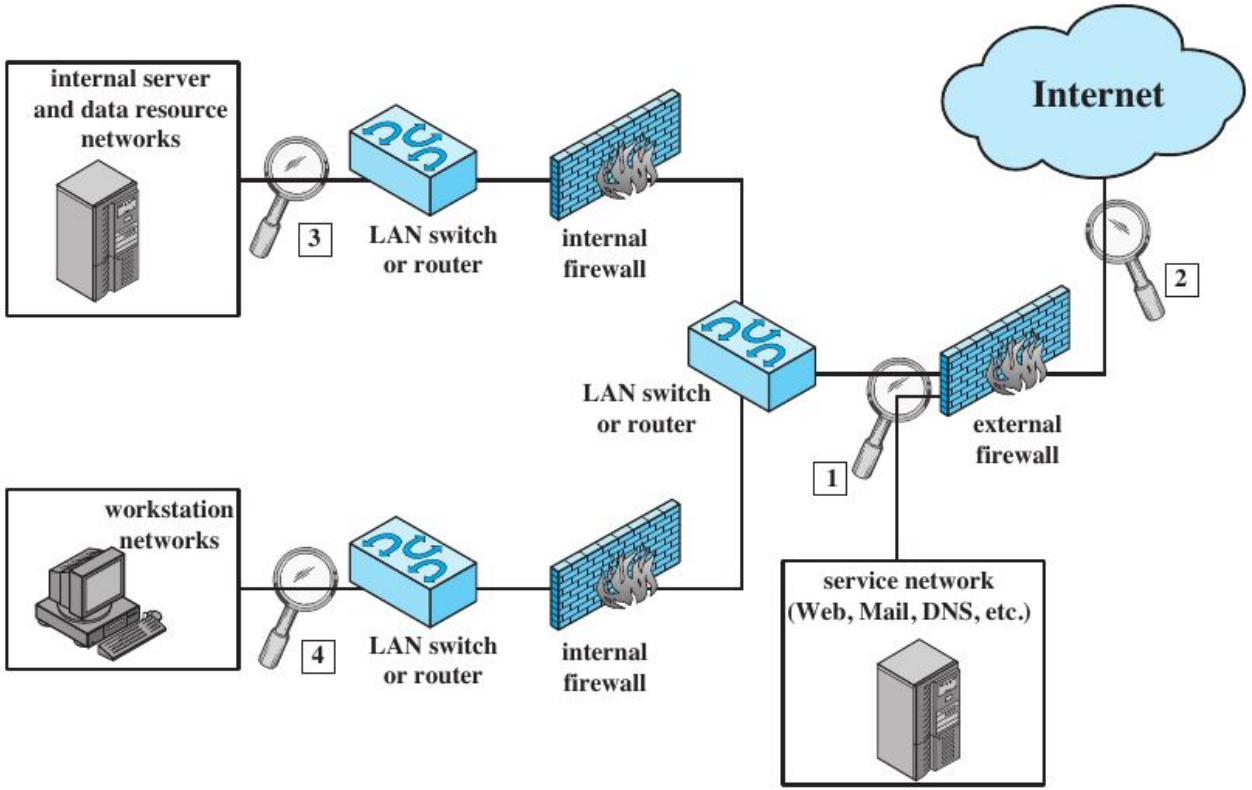
NIDS - Network Based IDS

- Monitoruje ruch w wybranych punktach sieci
- Bada pakiet po pakiecie w czasie rzeczywistym lub zbliżonym do czasu rzeczywistego
- Może badać aktywność protokołów na poziomie sieci, transportu i/lub aplikacji
- Składa się z wielu czujników, co najmniej jednego serwera do zarządzania NIDS oraz co najmniej jednej konsoli zarządzającej z interfejsem użytkownika
- Analiza wzorców ruchu może odbywać się na czujniku lub serwerze zarządzania

Czujniki (sensory) inline (aktywne) - mogą zablokować atak

Czujniki pasywne - są na ogół szybsze

NIDS - rozmieszczenie sensorów



NIDS - lokalizacja czujników

Czujnik 1:

- ataki pochodzące z zewnątrz (zewnętrzną zaporę sieciową)
- problemy związane z zasadami przyjętymi dla zapory sieciowej lub jej działaniem
- ataki, które mogą być wycelowane w serwer WWW lub serwer ftp.
- DS może czasami rozpoznać w ruchu wychodzącym znamiona ataku na serwer

NIDS - lokalizacja czujników

Czujnik 2:

- czujnik może monitorować cały, niefiltrowany ruch sieciowy
- dokumentuje liczbę ataków powstających w Internecie, wycelowanych w daną sieć.
- dokumentuje rodzaje powstających w Internecie ataków

NIDS - lokalizacja czujników

Czujnik 3:

- czujnik do ochrony głównych sieci szkieletowych, takich jak te, które udostępniają zasoby wewnętrznych serwerów i baz danych
- monitorowanie dużej ilości ruchu w sieci, co zwiększa możliwość dostrzegania ataków.
- wykrywanie nieupoważnionych działań wykonywanych przez legalnych użytkowników w granicach organizacji objętych zabezpieczeniami

NIDS - lokalizacja czujników

Czujnik 4:

- wykrywa ataki skierowane przeciw krytycznym systemom i zasobom
- umożliwia skoncentrowanie ograniczonych zasobów na aktywach sieciowych, których wartość jest oceniana najwyżej

Sposoby wykrywania włamań

Sposoby wykrywania włamań

Wykrywanie sygnatur:

- analiza protokołów warstwy aplikacji - przepełnienia buforów, odgadywanie haseł i przesyłanie szkodliwego oprogramowania
- analiza protokołów warstwy transportowej - nietypowe fragmentowanie pakietów, wyszukiwanie podatnych portów i ataki specyficzne dla protokołu TCP
- analiza protokołów warstwy sieciowej - fałszowane adresy IP i niedopuszczalne wartości nagłówka IP
- nieoczekiwane usługi aplikacji - host bezprawnie wykonujący jakąś usługę aplikacji

Sposoby wykrywania włamań

Wykrywanie anomalii:

- natężeniu ruch - ataki DoS
- skanowanie - warstwa aplikacji, warstwa transportowa, warstwa sieciowa
- robaki - anomalny ruch między hostami, anomalne porty, skanowanie

SPA - Stateful Protocol Analysis

Stanowa analiza protokołu - identyfikuje odchylenia stanu protokołu podobnie do metody opartej na anomali, ale wykorzystuje z góry określone uniwersalne profile oparte na „przyjętych definicjach łagodnej aktywności” opracowanych przez dostawców.

Przykład: monitorowanie żądań wraz z odpowiadającymi im odpowiedziami; każde żądanie powinno mieć przewidywalną odpowiedź, a te odpowiedzi, które wykraczają poza oczekiwane wyniki, będą oznaczane i dalej analizowane.

Główna wada to znaczne zapotrzebowanie na zasoby