Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

IR EXCELLENCE IN RESEARCH

Wydział Informatyki

WPROWADZENIE DO SYSTEMÓW ZABEZPIECZEŃ

dr hab. inż. Jerzy Pejaś, prof. ZUT

Wydział Informatyki

Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie

1

O czym będzie mowa w tym wykładzie?

AGENDA

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Informacje o przedmiocie wykładu

INFORMACJE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Organizacja wykładu i ćwiczeń z ZIO.
- **Cel wykładu:**
  Student powinien: (a) potrafić krytycznie wyjaśnić pojęcie zaufania w odniesieniu do systemów operacyjnych, zaufanych urządzeń oraz wymagań wobec tych urządzeń, (b) znać rolę i cel każdego komponentu modułu zaufanej platformy (TPM), (c) potrafić korzystać z wybranych interfejsów użytkownika (m.in. TSS API) do interakcji z TPM, (d) rozumieć, w jaki sposób technologie wirtualizacji mogą być łączone z zaufanymi modułami platformy w celu zbudowania zaufanej infrastruktury, (e) potrafić opisać niektóre architektury systemów, które dzięki zastosowaniu możliwości technologii TPM pozwalają na uzyskanie innowacyjnych i silnie zabezpieczonych rozwiązań.
- **Efekty kształcenia:**
  Student powinien: (a) znać zasady działania, instalowania i konfigurowania sprzętowych i wirtualnych modułów zaufanych platform, bezpiecznych systemów operacyjnych oraz ich wykorzystania w budowaniu zaufania do komponentów programowo-sprzętowych oraz architektur systemów, (b) potrafić instalować i konfigurować sprzętowe i wirtualne moduły zaufanych platform, bezpieczne systemy operacyjne oraz posiadać umiejętność programowania wirtualnych i sprzętowych modułów zaufanych platform.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

3

Informacje o treści wykładów

INFORMACJE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Wprowadzenie do systemów zabezpieczeń
- Zaufanie i zabezpieczenia
- Bezpieczne obliczenia oparte na sprzęcie i oprogramowaniu
- Główne źródło zaufania
- Trusted Platform Module (TPM)
- Podstawowe funkcje modułu TPM
- Zaufana wirtualizacja
- Zastosowania TPM
- Bezpieczny system operacyjny SELinux

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

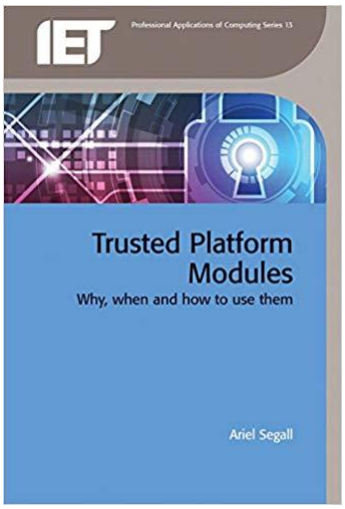
Wydział Informatyki

4

Literatura podstawowa

LITERATURA

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Ariel Segall *Trusted Platform Modules: Why, When and How to Use Them (Computing and Networks)*

  Institution of Engineering and Technology, 2017

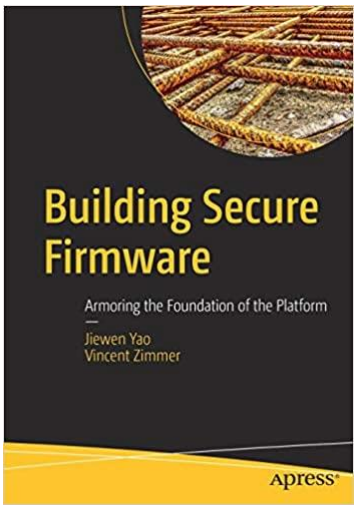
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Literatura podstawowa

LITERATURA

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Jiewen Yao, Vincent Zimmer: *Building Secure Firmware - Armoring the Foundation of the Platform*. ISBN 978-1-4842-6105-7, pp. 1-930

  Apress 2020

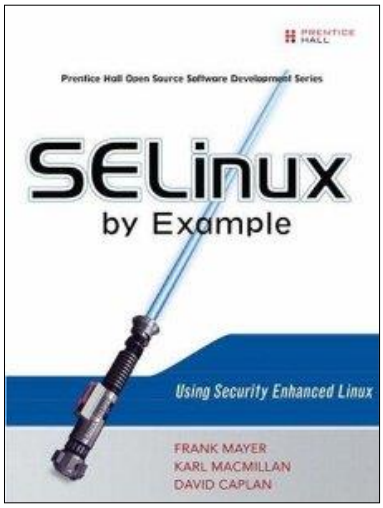
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Literatura podstawowa

LITERATURA

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Frank. Mayer, Karl MacMillan, David Caplan *SELinux by Example: Using Security Enhanced Linux*

  Prentice Hall, 2006

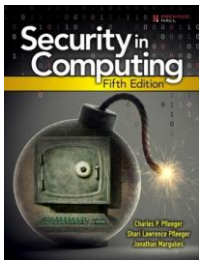
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Literatura dodatkowa

LITERATURA

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

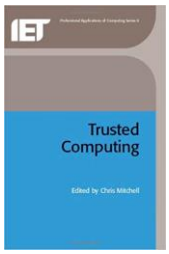


- Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies *Security in Computing*

  Pearson Education, 5th Edition, 2015

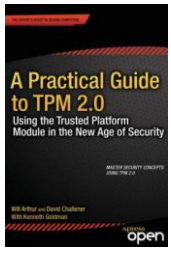
- Graeme Proudler, Liqun Chen, Chris Dalton *Trusted Computing Platforms*

  Springer Cham Heidelberg New York Dordrecht London 2014



- Chris Mitchell *Trusted Computing (Computing and Networks)*

  The Institution of Engineering and Technology, 2005



- W. Arthur , D. Challener A Practical Guide to TPM 2.0 - Using the Trusted Platform Module in the New Age of Security

  Apress Open, 2015

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Literatura dodatkowa

LITERATURA

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- S. W. Smith *Trusted Computing Platforms: Design and Applications*, Springer Verlag, 2005
- S. Kinney *Trusted Platform Module Basics Using TPM in Embedded Systems*, Elsevier, 2006
- D. Challener, L. Van Doorn, D. Safford, K. Yoder, R. Catherman *A Practical Guide to Trusted Computing*, IBM Press, 2007
- B. McCarty *SELinux*, O'Reilly, 2004
- Carlisle Adams, Steve Lloyd *PKI. Podstawy i zasady działania*, Wyd. Naukowe PWN, 2007
- Wolfgang Rankl, Wolfgang Effing *Smart Card Handbook*, John Wiley and Sons, Ltd.

Literatura dodatkowa – TPM 2.0 Software Stack (TSS)

LITERATURA

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- TCG TSS 2.0 Overview and Common Structures Specification
- TCG TSS 2.0 TPM Command Transmission Interface (TCTI) API Specification
- TCG TSS 2.0 Marshaling/Unmarshaling API Specification
- TCG TSS 2.0 System API (SAPI) Specification
- TCG TSS 2.0 Enhanced System API (ESAPI) Specification
- TCG TSS 2.0 Feature API (FAPI) Specification
- TCG TSS 2.0 TAB and Resource Manager Specification

Literatura dodatkowa – TPM 2.0 Library

LITERATURA

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- TPM Library Part 1: Architecture
- TPM Library Part 2: Structures
- TPM Library Part 3: Commands
- TPM Library Part 3: Commands – Code
- TPM Library Part 4: Supporting Routines
- TPM Library Part 4: Supporting Routines – Code

Konspekty do wykładu

AGENDA

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Konspekty wykładów oraz inne materiały związane z kursem Zaufana Infrastruktura Obliczeniowa (m. in. zasady zaliczeń) dostępne są na platformie MS Teams w zespole:

"22/23, 2L, NII, Zaufana infrastruktura obliczeniowa, informatyka, wykład, N2_I_PO_W_11, WI, 3961298"

katalog: "Materiały z zajęć"

Motto

POJĘCIA ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

Any data management issue is a security issue!

Trust, Privacy, and Security
Summary of a Workshop Breakout Session at the National Science Foundation Information and Data Management (IDM) Workshop held in Seattle, Washington, September 14 - 16, 2003

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Co to jest bezpieczeństwo komputera?

POJĘCIA ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Jest to ochrona zasobów systemu komputerowego
  - sprzętu komputerowego: komputer, urządzenia (sterownik dysku, pamięć, drukarka), sprzęt sieciowy
  - oprogramowania: system operacyjny, użytkowe, (antywirus), aplikacje komercyjne (procesory tekstu, edytory obrazów), aplikacje użytkownika
  - danych: dokumenty, zdjęcia, muzyka, video, e-maile, projekty
- Krótko: zapewnienie komputerowi odpowiednich właściwości bezpieczeństwa, np. CIA (Confidentiality, Integrity and Availability)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

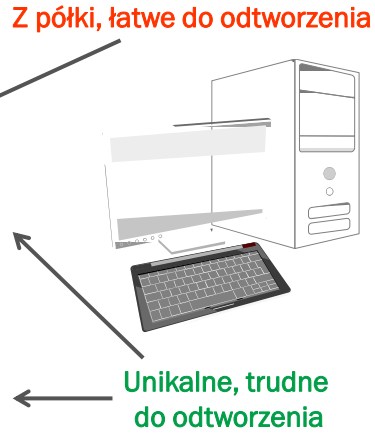
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

Co to jest bezpieczeństwo komputera?

BEZPIECZEŃSTWO ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Ochrona zasobów systemu komputerowego
  - sprzętu komputerowego: komputer, urządzenia (sterownik dysku, pamięć, drukarka), sprzęt sieciowy
  - oprogramowania: system operacyjny, użytkowe, (antywirus), aplikacje komercyjne (procesory tekstu, edytory obrazów), aplikacje użytkownika
  - danych: dokumenty, zdjęcia, muzyka, video, e-maile, projekty



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Podatności, zagrożenia, ataki, kontrolowanie

PODATNOŚĆ ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Podatność jest słabością systemu bezpieczeństwa powstałą na etapie opracowywania procedur, projektowania lub implementacji, które mogą przyczynić się do powstania straty lub szkody.
- Zagrożeniem systemu komputerowego jest zestaw okoliczności, które mogą spowodować straty lub szkody
  - potencjalne naruszenie bezpieczeństwa
- Adwersarz (przestępca): osoba, która wykorzystuje podatność do przeprowadzenia ataku na system.
- Jak rozwiązać te problemy?
  - Zastosować kontrolowanie jako środek zaradczy
  - Oznacza to, że kontrolowanie jest działaniem, urządzeniem, procedurą lub techniką, która usuwa lub zmniejsza podatność.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

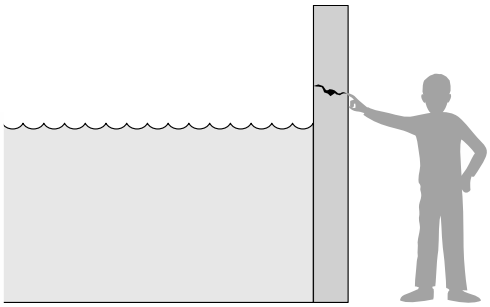
Zagrożenie i podatność

KONTROLOWANIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Związek między podatnościami, zagrożeniami i kontrolowaniem:
  - Zagrożenie jest blokowane przez kontrolowanie podatności.
  - Aby kontrolowanie było skuteczne musimy wiedzieć jak najwięcej o zagrożeniach.

Fakt, że może wystąpić naruszenie bezpieczeństwa (zagrożenie) oznacza, że należy zabezpieczyć się przed działaniami, które mogą je spowodować.



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Cele zabezpieczeń aktywów: triada CIA (Confidentiality, Integrity, Availability)

CIA ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Zabezpieczenia (nie tylko komputera) dotyczą trzech ważnych aspektów związanych z aktywami każdego systemu komputerowego:
  - **Poufność** (ang. confidentiality): atakujący nie powinien być w stanie wejść w posiadanie informacji dotyczących systemu lub jego użytkowników.
  - **Integralność** (ang. integrity): system powinien nadal działać prawidłowo, o ile tylko osiągnie stany, które wystąpiłyby w przypadku nieobecności atakującego
  - **Osiągalność**, **dostępność** (ang. availability): działania podejmowane przez atakującego nie uniemożliwiają użytkownikom korzystania z systemu.
- Pod uwagą mogą być brane także inne aspekty, np.:
  - **Uwierzytelnienie** (ang. authentication): proces lub działanie polegające na udowodnieniu lub pokazaniu czegoś, co jest prawdziwe, autentyczne lub ważne.
  - **Niezaprzeczalność** (ang. nonrepudiation): jest zapewnienie, że ktoś nie może zaprzeczyć podjętym działaniom lub złożonym deklaracjom

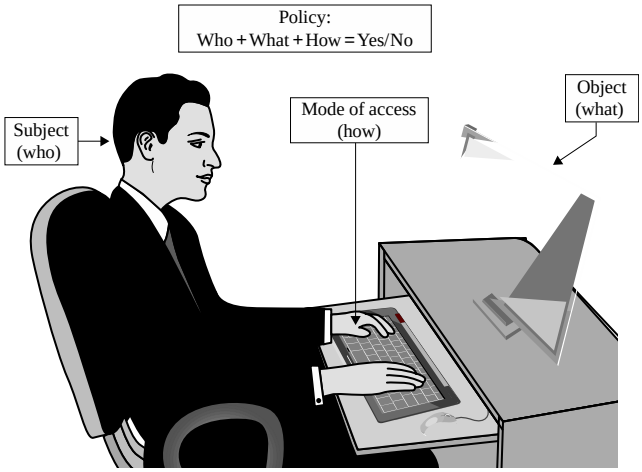
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Konrola dostępu

KONTROLA ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



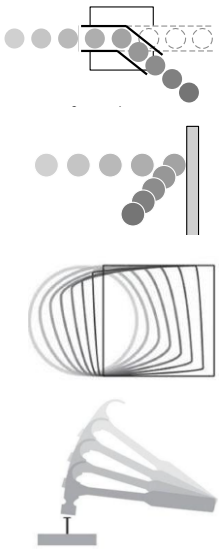
Charles P. Pfleeger i inni. *Security in Computing, Fifth Edition,* 2015 Pearson Education, Inc.

Zagrożenia

ZAGROŻENIA ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Przechwycenie oznacza, że niektóre nieupoważnione podmioty uzyskały dostęp do aktywów.
- W wyniku przerwania składnik systemu zostaje utracony, niedostępny lub nie nadaje się do użytku.
- Jeśli nieupoważniona strona nie tylko uzyskuje dostęp, ale także manipuluje (fałszuje) zasób, to zagrożenie to jest nazywane modyfikacją.



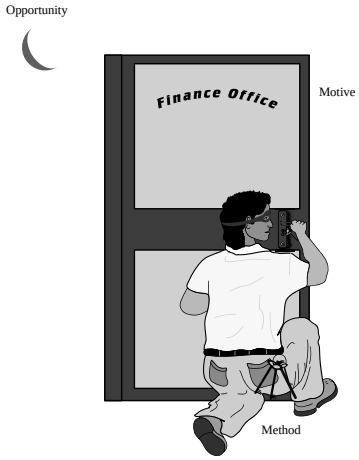
- Wreszcie, nieupoważniona strona może tworzyć fałszywe obiekty w systemie komputerowym.

Metoda — okazja — motyw (MOM, Method — Opportunity — Motive)

MOM ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Złośliwy atakujący musi mieć **trzy elementy (MOM)**:
  - **metodę**: umiejętności, wiedza, narzędzia i inne elementy, dzięki którym można przeprowadzić atak
    - wiedza na temat systemów systemów jest powszechnie dostępna
  - **okazję**: odpowiedni moment i dostęp do systemu, który jest celem ataku
    - do systemów dostępnych publicznie dostęp maja także intruzi
  - **motyw**: powód, dla którego intruz chce wykonać atak przeciwko określonemu systemowi



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

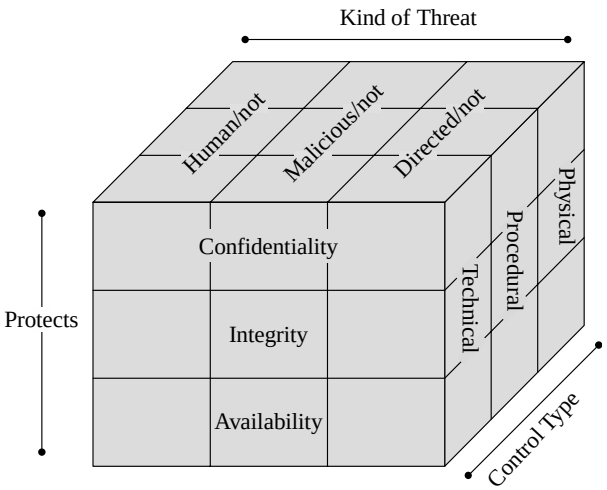
Wydział Informatyki

Charles P. Pfleeger i inni. *Security in Computing, Fifth Edition,* 2015 Pearson Education, Inc.

Kontrolowanie/środki zaradcze

KONTROLOWANIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Charles P. Pfleeger i inni. *Security in Computing, Fifth Edition,* 2015 Pearson Education, Inc.

Cele zabezpieczeń

KONTROLOWANIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Mówiąc o bezpieczeństwie komputerowym, mamy na myśli przede wszystkim jego trzy najważniejsze właściwości: poufność, integralność i dostępność (tzw. triada CIA)
- Poufność zapewnia, że dostęp do zasobów komputerowych mają tylko uprawnione podmioty:
  - dostęp dotyczy możliwości czytania, przeglądania, drukowanie, a nawet wiedzy o istnieniu tych zasobów;
  - zasoby są objęte tajemnicą lub prywatnością
- Integralność oznacza, że aktywa mogą być modyfikowane tylko przez uprawnione strony lub tylko w autoryzowany sposób:
  - dotyczy to m.in. pisania, usuwania, tworzenia
- Dostępność oznacza, że dostęp do zasobów w określonym czasie mają wszystkie upoważnione podmioty.
  - własność ta jest często rozumiana jako przeciwieństwo właściwości odmowa usługi (ang. Denial of Service).

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

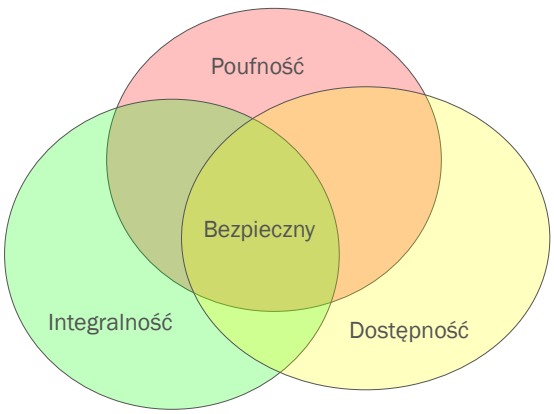
Charles P. Pfleeger i inni. *Security in Computing, Fifth Edition,* 2015 Pearson Education, Inc.

Zależność pomiędzy poufnością, integralnością a dostępnością

KONTROLOWANIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- W praktyce te trzy właściwości mogą być niezależne, mogą się pokrywać, a nawet wykluczać.



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Charles P. Pfleeger i inni. *Security in Computing, Fifth Edition,* 2015 Pearson Education, Inc.

Funkcje zabezpieczeń

CELE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Zapobieganie
  - Zapobiegaj atakom naruszającym politykę bezpieczeństwa
- Wykrywanie
  - Wykryj naruszenie polityki bezpieczeństwa przez atakujących
- Odtwarzanie
  - Zatrzymaj atak, oceń i napraw uszkodzenia
  - Kontynuuj prawidłowe działanie, nawet jeśli atak się powiedzie

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zaufanie i założenia

ZAUFANIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Zaufanie leży u podstaw wszystkich aspektów bezpieczeństwa
- Polityki
  - Jednoznacznie wyróżniają stany systemu
  - Prawidłowo definiują wymagania bezpieczeństwa
- Mechanizmy
  - Konieczne do egzekwowania polityk bezpieczeństwa
  - Przyjmuje się, że mechanizmy wsparcia działają poprawnie

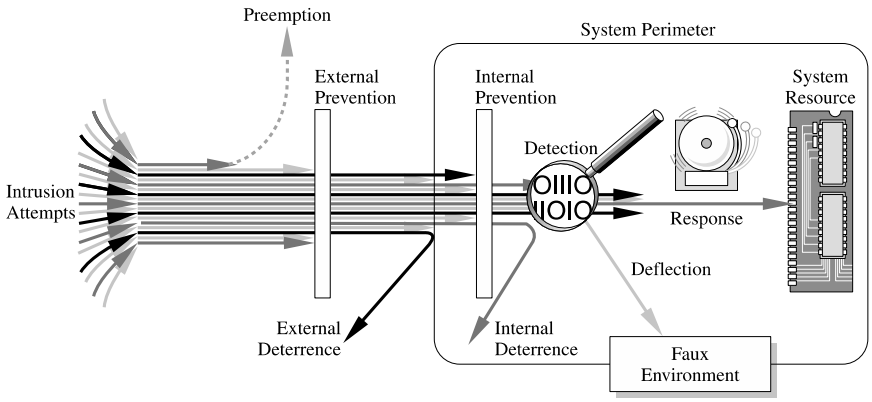
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Różne typy kontrolowania

TYPY ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



Charles P. Pfleeger i inni. *Security in Computing, Fifth Edition,* 2015 Pearson Education, Inc.

Dostępne elementy kontrolujące

ELEMENTY ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Szyfrowanie
  - Przyjmujemy dane w ich normalnym, nieszyfrowanym stanie, zwanym
    - tekstem jawnym i przekształcamy je tak, aby były niezrozumiałe i niemożliwe do odtworzenia do postaci jawnej przez zewnętrznego obserwatora; przekształcone dane nazywane są zaszyfrowanym tekstem lub tekstem niejawnym.
  - Szyfrowanie praktycznie zaspokaja potrzebę zachowania poufności danych.
  - Ponadto szyfrowanie można wykorzystać do zapewnienia integralności;
    - danych, których na ogół nie można odczytać, nie można łatwo zmienić w taki sposób, że zmienione dane mają sens.

Dostępne elementy kontrolujące (c.d.)

ELEMENTY ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Szyfrowanie nie rozwiązuje wszystkich problemów związanych z bezpieczeństwem komputera; stąd potrzebne są inne narzędzia i techniki, które muszą uzupełniać jego użycie.
  - jeśli szyfrowanie stosowane jest niewłaściwie, to może nie mieć wpływu na bezpieczeństwo, co więcej może nawet obniżyć wydajność całego systemu.
- Słabe szyfrowanie może być gorsze niż brak szyfrowania,
  - ponieważ daje użytkownikom nieuzasadnione poczucie bezpieczeństwa.
- Dlatego musimy rozumieć sytuacje, w których szyfrowanie jest najbardziej przydatne, a także sposoby jego skutecznego wykorzystania.

Dostępne elementy kontrolujące (c.d.)

ELEMENTY ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Kontrola oprogramowania/programu
  - Programy muszą być wystarczająco bezpieczne, aby zapobiec atakowi z zewnątrz
  - Powinny być także rozwijane i utrzymywane tak, abyśmy byli pewni ich rzetelności.
- Elementy kontrolne programu obejmują:
  - Wewnętrzna kontrola programu: części programu, które egzekwują zasady bezpieczeństwa i wynikające z tego ograniczenia,
    - np. ograniczenia dostępu w programie do zarządzania bazą danych
  - System operacyjny i kontrola systemu sieciowego: ograniczenia narzucone przez system operacyjny lub sieć w celu ochrony każdego użytkownika przed innymi użytkownikami
    - tj. chmod w systemie UNIX: (odczyt, zapis, wykonanie) vs. (właściciel, grupa, inne)
  - Niezależne programy kontrolne: programy aplikacyjne,
    - np. weryfikatory haseł, narzędzia do wykrywania włamań lub skanery antywirusowe, które chronią przed niektórymi rodzajami podatności

Dostępne elementy kontrolujące (c.d.)

ELEMENTY ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Kontrolowanie wytwarzania oprogramowania:
  - standardy jakości, zgodnie z którymi program jest tak projektowany, implementowany, testowany i utrzymywany, aby zapobiec defektom oprogramowania, które mogą zostać wykorzystane jako podatności
    - np. testy penetracyjne (nazywane też pen testami lub etycznym hakowaniem) to praktyka testowania systemu komputerowego, sieci lub aplikacji internetowej w celu wykrycia luk w zabezpieczeniach, które może wykorzystać osoba atakująca.
- Kontrola oprogramowania często wpływa bezpośrednio na użytkowników
  - np. wtedy, gdy użytkownik podczas pracy zostanie zapytany o hasło przed uzyskaniem dostępu do programu lub danych;
  - ponieważ wpływa to na użyteczność systemu, kontrolowanie oprogramowania musi być starannie zaprojektowane;
    - łatwość użycia i możliwości są często sprzecznymi celami podczas projektowania mechanizmów kontrolowania oprogramowania.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Dostępne elementy kontrolujące (c.d.)

ELEMENTY ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Kontrolowanie sprzętowe
  - Stworzono wiele urządzeń, które wspomagają bezpieczeństwo komputera. Urządzenia te obejmują różne środki, takie jak
    - szyfrowanie sprzętowe lub z wykorzystaniem inteligentnych kart (ang. smart cards);
    - zamki lub linki (ang. cables) ograniczające dostęp lub zapobiegające kradzieży
    - urządzenia do weryfikacji tożsamości użytkowników;
    - śluzy bezpieczeństwa (ang. firewalls);
    - systemy wykrywania włamań (IDS)
    - płytki drukowane kontrolujące dostęp do nośników pamięci.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Częste podatności oprogramowania

PODATNOŚCI ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Brak sprawdzanie poprawności danych wejściowych
- Przepełnienie bufora
- Problemy z formatowaniem łańcucha
- Przepełnienie rejestru liczb całkowitych
- Warunki wyścigu
- itp...

Przepełnienie bufora - pojęcia

BUFOR ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Co to jest przepełnienie bufora?
  - Program alokuje ciągły obszar pamięci o ustalonym rozmiarze, wykorzystywany do przechowywania danych (tzw. bufor)
  - Kopiowana do bufora liczba danych przekracza jego pojemność, co powoduje nadpisanie innych obszarów pamięci
- Dlaczego jest to tak istotny problem?
  - Wiele krytycznych programów jest pisanych w C/C++...
  - ... ale C/C++ w czasie wykonywania nie kontroluje ograniczeń nakładanych na pamięć.

Przepełnienie bufora

BUFOR ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Przepełnienie stosu
  - Kod powłoki
  - Powrót do libc
    - Przepełnienie ustawia adres powrotu na adres funkcji libc
  - O jedne bajt za daleko
  - Wskaźniki funkcji przepełnienia i bufory longjmp
- Przepełnienie sterty

Program podatny na atak

ATAK ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

Program podNaAtak.c

```
#include <stdio.h>
main(void) {
  char buffer[128];
  FILE* file;

  freopen("fifo", "r", stdin);
  gets(buffer);
}
```

`FILE *freopen( const char *path, const char *mode, FILE *stream);`

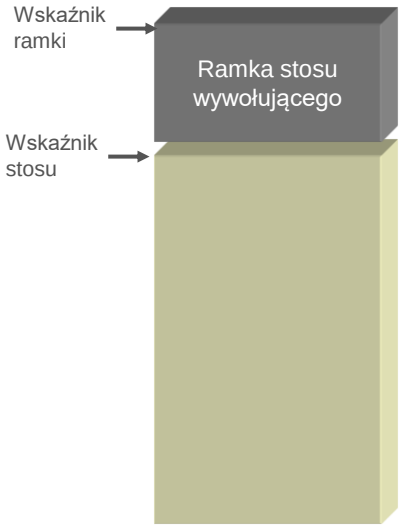
Funkcja **freopen** otwiera plik, którego nazwa jest zawarta w łańcuchu wskazywanym przez ***path*** i wiąże z nim strumień wskazywany przez ***stream***. Pierwotny strumień jest zamykany (jeśli istnieje). Argument *mode* ma takie samo znaczenie jak w przypadku funkcji fopen.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Wydział Informatyki
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

Przepełnienie bufora (1/9) [2022-10-05]

PRZEPEŁNIENIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Wywołujący wykonuje
  push return address;
- Wywołana procedura wykonuje

```
push fp;
fp := sp;
// alokacja pamięci na bufor
sp := sp - sizeof(buffer);
gets(buffer);
// powrót z gets
sp := fp;
fp := pop();
pc := pop();
```

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

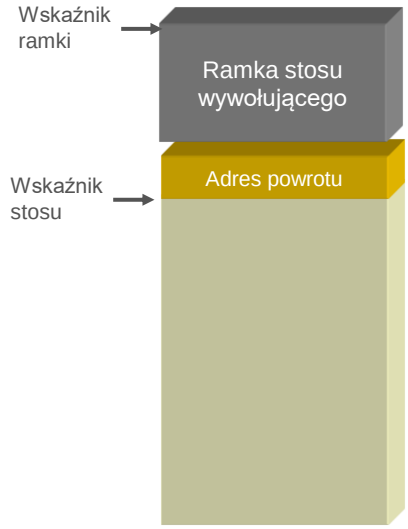
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

37

Przepełnienie bufora (2/9)

PRZEPEŁNIENIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Wywołujący wykonuje
  push return address;
- Wywołana procedura wykonuje

```
push fp;
fp := sp;
// alokacja pamięci na bufor
sp := sp - sizeof(buffer);
gets(buffer);
// powrót z gets
sp := fp;
fp := pop();
pc := pop();
```

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

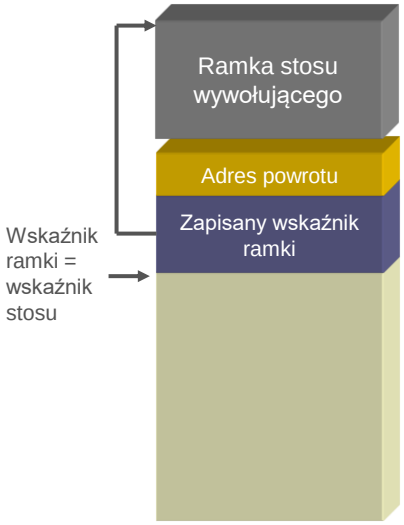
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

38

Przepełnienie bufora (3/9)

PRZEPEŁNIENIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Wywołujący wykonuje
  - push return address;
- Wywołana procedura wykonuje

```
push fp;
fp := sp;
// alokacja pamięci na bufor
sp := sp - sizeof(buffer);
gets(buffer);
// powrót z gets
sp := fp;
fp := pop();
pc := pop();
```

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

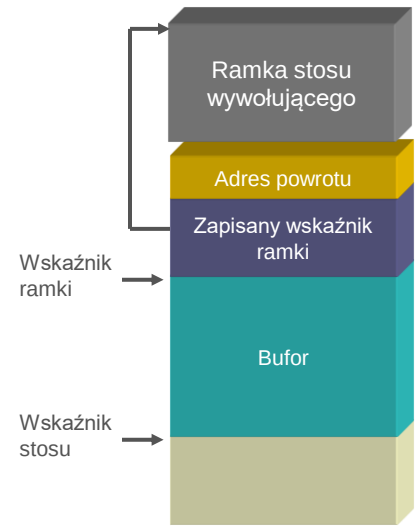
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

39

Przepełnienie bufora (4/9)

PRZEPEŁNIENIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Wywołujący wykonuje
  - push arg1; . . . ; push argN;
  - push return address;
- Wywołana procedura wykonuje

```
push fp;
fp := sp;
// alokacja pamięci na bufor
sp := sp - sizeof(buffer);
gets(buffer);
// powrót z gets
sp := fp;
fp := pop();
pc := pop();
```

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

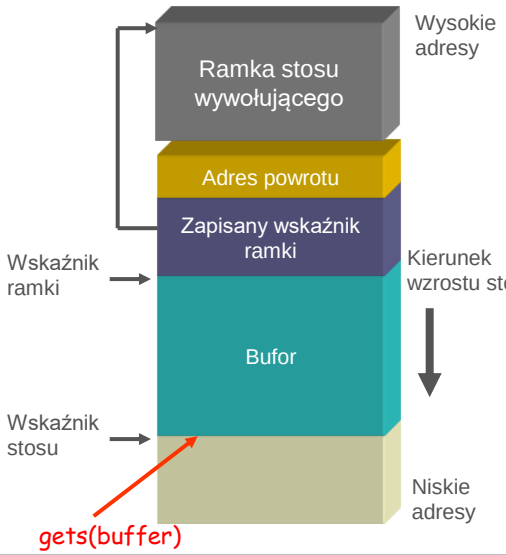
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

40

Przepełnienie bufora (5/9)

PRZEPEŁNIENIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Wywołujący wykonuje
  push arg1; . . . ; push argN;
  push return address;
- Wywołana procedura wykonuje
  push fp;
  fp := sp;
  // alokacja pamięci na bufor
  sp := sp - sizeof(buffer);
  gets(buffer);
  // powrót z gets
  sp := fp;
  fp := pop();
  pc := pop();

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

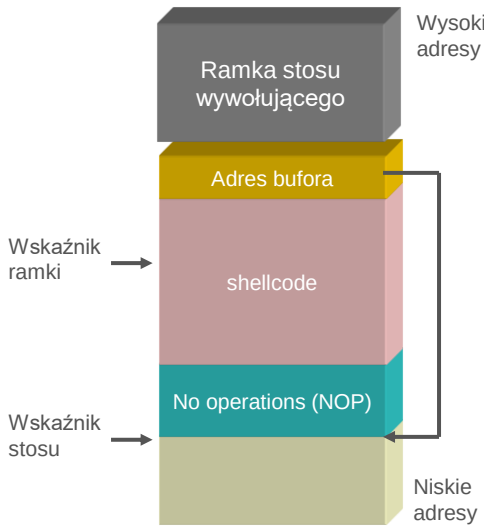
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

41

Przepełnienie bufora (6/9)

PRZEPEŁNIENIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Wywołujący wykonuje
  push arg1; . . . ; push argN;
  push return address;
- Wywołana procedura wykonuje
  push fp;
  fp := sp;
  // alokacja pamięci na bufor
  sp := sp - sizeof(buffer);
  gets(buffer);
  // powrót z gets
  sp := fp;
  fp := pop();
  pc := pop();

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

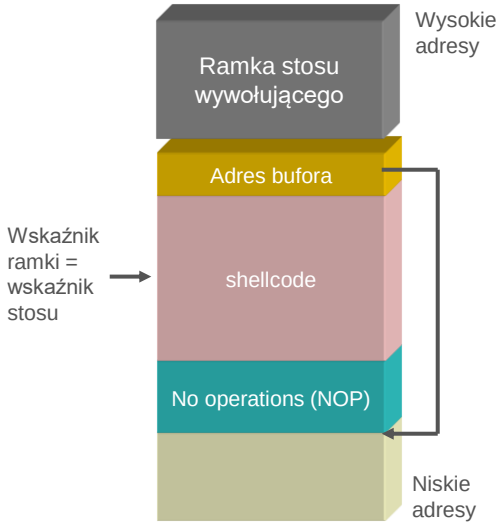
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

42

Przepełnienie bufora (7/9)

PRZEPEŁNIENIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Wywołujący wykonuje
  push arg1; . . . ; push argN;
  push return address;
- Wywołana procedura wykonuje

```
push fp;
fp := sp;
// alokacja pamięci na bufor
sp := sp - sizeof(buffer);
gets(buffer);
// kod procedury
sp := fp;
fp := pop();
pc := pop();
```

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

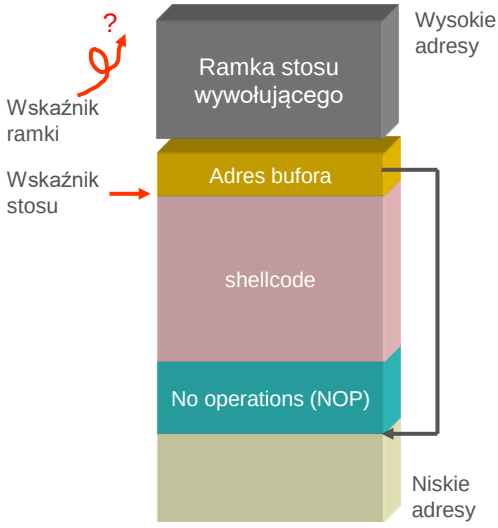
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

43

Przepełnienie bufora (8/9)

PRZEPEŁNIENIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Wywołujący wykonuje
  push arg1; . . . ; push argN;
  push return address;
- Wywołana procedura wykonuje

```
push fp;
fp := sp;
// alokacja pamięci na bufor
sp := sp - sizeof(buffer);
gets(buffer);
// kod procedury
sp := fp;
fp := pop();
pc := pop();
```

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

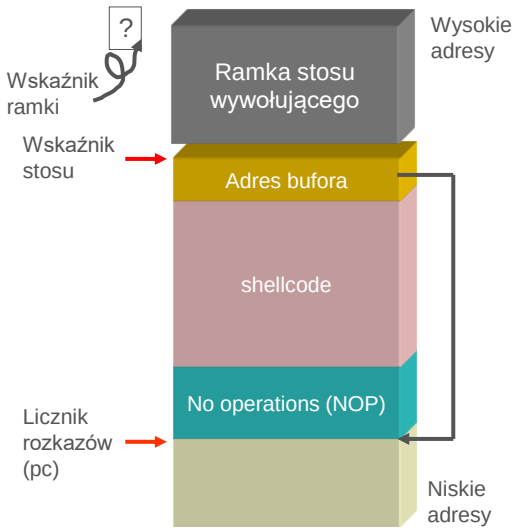
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

44

Przepełnienie bufora (9/9)

PRZEPEŁNIENIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



- Wywołujący wykonuje
  push arg1; . . . ; push argN;
  push return address;
- Wywołana procedura wykonuje

```
push fp;
fp := sp;
// alokacja pamięci na bufor
sp := sp - sizeof(buffer);
gets(buffer);
// kod procedury
sp := fp;
fp := pop();
pc := pop();
```

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Modyfikacja wykonania procesu

PRZYKŁAD ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

```
void function() {
        char buffer1[4];
        int *ret;
        ret = (int *)(buffer1 + 8);
        (*ret) += 7;
}
```

```
void main() {
    int x = 0;
  function();
    x = 1;
  printf ("%d\n",x);
}
```

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

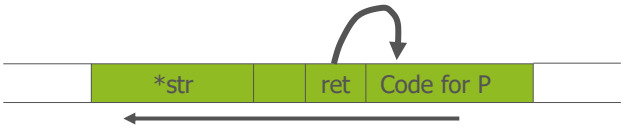
Wydział Informatyki

RETURN-TO-LIBC ATTACK ...

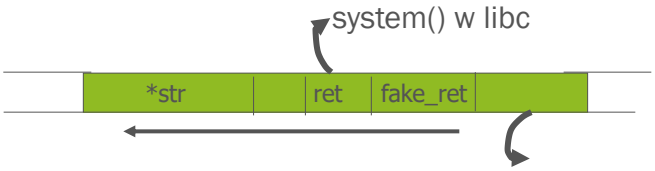
- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

Atak na adres powrotu do funkcji libc (ang. return-to-libc attack)

Obejście niewykonywalnego stosu za pomocą kontekstowego wykorzystania wytrychu (ang. exploit) return-to-libc



Atak za pomocą shell code: Program P: `exec( "/bin/sh" )`



Atak return-to-libc:

ZAPOBIEGANIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

Zapobieganie atakom przepełnienia bufora

- Używaj bezpiecznych języków (Java, Meta Language ML).
- Używaj bezpiecznych funkcji bibliotecznych
- Statyczna analiza kodu źródłowego.
- Niewykonalny stos
- Sprawdzanie w czasie wykonywania programu (ang. runtime): StackGuard, Libsafe, SafeC, Purify.
- Randomizacja przestrzeni adresowej.
- Wykrywanie anomalii w zachowaniu programu
- Kontrola dostępu do informacji o skutkach ataków...

Sprawdzanie w czasie wykonywania programu: StackGuard

STACKGUARD ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

Istnieje wiele technik sprawdzania programu w czasie czasu wykonywania...

StackGuard testuje integralność stosu.

Osadź „canaries” w ramce stosu i sprawdź ich integralność przed powrotem z wywoływanej funkcji.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zagrożenia

ZAUFANE OBLICZENIA ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Gdy atakowane są komputery i ich użytkownicy:
  - instalujemy łatki
  - aktualizujemy oprogramowanie antywirusowe
  - uruchomiamy oprogramowanie antyszpiegowskie
  - ponownie instalujemy poprawki
  - sprawdzamy aktualizacje
  - pobieramy łatki ...
  - ... i mamy nadzieję, i modlimy się ...
- Ale dlaczego nie tworzyć bezpiecznego oprogramowania?
  - Ludzie o to nie dbają (przynajmniej tak się wydaje); bezpieczeństwo przeszkadza i sprawia, że korzystanie z komputerów jest bardziej kłopotliwe;
- Pisanie bezpiecznego oprogramowania wymaga dobrze wykształconych programistów.
- Zaufane obliczenia (ang. Trusted Computing) może pomóc przerwać cykl, o którym była mowa wyżej, o ile będziemy postępować inaczej. O tym dalej!

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zidentyfikowane wymagania badawcze dotyczące zaufanych komputerów

ZAUFANE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

Wymaganie	Wymagania badawcze	Komentarz
Izolacja programów	Rozdzielenie domen Obsługa nieoczekiwanych wydarzeń	Izolacja jest taka sama jak separacja domen. Izolacja może zapewnić mechanizm obsługi nieprzewidzianych zdarzeń.
Oddzielenie użytkownika od przełożonego	Oddzielenie użytkownika od przełożonego	Wymagania dotyczące zaufanej platformy odpowiadają wymaganiom badawczym
Bezpieczne długookresowe przechowywanie		Oryginalne badania wskazują na potrzebę długo okresowego, chronionego przechowywania.
Identyfikacja bieżącej konfiguracji		Oryginalne badania zakładają, że określenie tożsamości platformy nie stanowi żadnego problemu.
Weryfikowalny raport o bieżącej konfiguracji		Bez problemów z tożsamością i przy założeniu bezpiecznego dostarczania oprogramowania, nie ma potrzeby raportowania konfiguracji platformy.
Sprzętowa baza ochrony	Sprzętowa baza ochrony	Wymagania dotyczące zaufanej platformy odpowiadają wymaganiom badawczym

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zaufanie

ZAUFANIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Zaufanie: mierzalne przekonanie i/lub wiara, które reprezentują skumulowaną wartość historyczną i wartość oczekiwaną w przyszłości.
- UWAGA - Zaufanie jest obliczane ilościowo i/lub jakościowo i mierzone. Zaufanie służy do oceny wartości podmiotów, łańcuchów wartości łączących wielu interesariuszy i ludzkich zachowań, w tym podejmowanych decyzji.

ITU-T Y.3052 *Overview of trust provisioning in information and communication technology infrastructures and services, 2017*

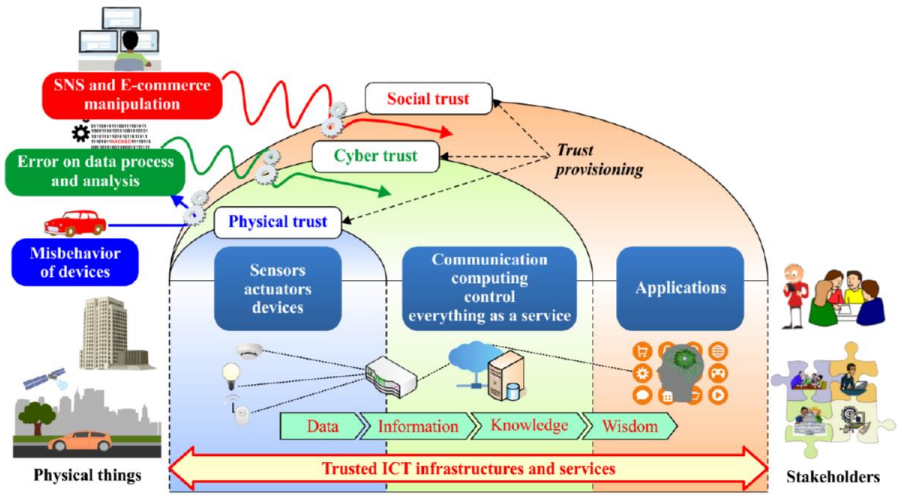
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zaufane infrastruktury i usługi ICT

INFRASTRUKTURA ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



ITU-T Y.3052 *Overview of trust provisioning in information and communication technology infrastructures and services, 2017*

Zaufanie fizyczne

ZAUFANIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Zaufanie fizyczne odzwierciedla różne aspekty zaufania do rzeczy fizycznych, które można zmierzyć biorąc pod uwagę ich wiarygodność z punktu widzenia możliwości, integralności i współpracy.
  - Możliwość oznacza zdolność rzeczy fizycznej do wykonania zadania zgodnie z założoną funkcjonalnością.
  - Integralność oznacza stan rzeczy fizycznej, w którym działa stabilnie bez kłopotów i awarii.
  - Współpraca oznacza, że rzecz fizyczna współpracuje z innymi rzeczami fizycznymi realizując wspólne cele.
- Zaufanie fizyczne odzwierciedla skłonność do zaufania rzeczy fizycznej, na którą wpływ mają zagrożenia związane ze światem fizycznym.

ITU-T Y.3052 *Overview of trust provisioning in information and communication technology infrastructures and services, 2017*

Cyberzaufanie

ZAUFANIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Cyberzaufanie odzwierciedla różne aspekty zaufania do cyberobiektów, które można zmierzyć biorąc pod uwagę ich wiarygodność z punktu widzenia możliwości, integralności i współpracy.
  - Możliwość zdolność oznacza, że zdolność cyberobiektu jest prawidłowa i pewna z punktu widzenia wykonywania kontroli, obliczeń i komunikacji.
  - Integralność oznacza, że dane przetwarzane lub dostarczane przez cyberobiekty nie są przypadkowo lub złośliwie zmieniane lub niszczone podczas kontroli, obliczeń i komunikacji.
  - Współpraca określa, na ile dobrze cyberobiekt współpracuje z innymi obiektami.
- Cyberzaufanie odzwierciedla skłonność do zaufania cyberobiektom, na którą wpływ mają zagrożenia związane z cyberprzestrzenią.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ITU-T Y.3052 *Overview of trust provisioning in information and communication technology infrastructures and services, 2017*

Zaufanie społeczne

ZAUFANIE ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Zaufanie społeczne odzwierciedla różne aspekty zaufania do podmiotów społecznych. Można je mierzyć, biorąc pod uwagę wiarygodność jednostki z punktu widzenia umiejętności, uczciwości i życzliwości.
  - Umiejętność oznacza kompetencje człowieka niezbędne w jego indywidaulnych działaniach.
  - Uczciwość implikuje, że podmiot społeczny traktuje innych uczciwie.
  - Życzliwość oznacza, na ile uprzejmie zachowuje się podmiot społeczny w stosunku do innych podmiotów społecznych lub jak bardzo podmiot społeczny współdziała z innymi podmiotami zgodnie z ich potrzebami.
- Zaufanie społeczne odzwierciedla skłonność do zaufania, na którą wpływ mają zagrożenia w świecie społecznym.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

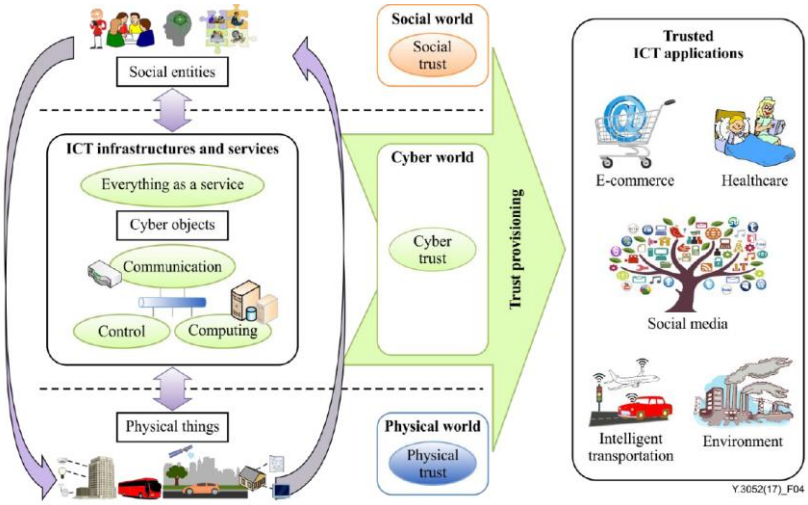
Wydział Informatyki

ITU-T Y.3052 *Overview of trust provisioning in information and communication technology infrastructures and services, 2017*

Model udostępniania zaufania

MODEL ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia



ITU-T Y.3052 *Overview of trust provisioning in information and communication technology infrastructures and services, 2017*

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

57

Definicja pojęcia Zaufane Obliczenia (ang. Trusted Computing)

DEFINICJA ...

- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Trusted Computing is the expectation that a device will behave in a particular manner for a specific purpose [TCG2004]

  Trusted Computing Group, *TCG Specification – Architecture Overview,* Rev. 1.2, 2004

- Trustworthiness is assurance that a system or a component will perform as expected.

  Committee on Information Systems Trustworthiness (1999): *Trust in Cyberspace*

- Zaufane obliczenia oznaczają wykonywanie oprogramowania o kluczowym znaczeniu dla bezpieczeństwa w systemie w taki sposób, że jeśli jego obecny status został sklasyfikowany jako godny zaufania (wiarygodny), to posiada ono odpowiednie środki konieczne do utrzymania tego statusu".

  Thomas Müller *Trusted Computing Systeme*

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

58

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

IR EXCELLENCE IN RESEARCH

Wydział Informatyki

DZIĘKUJĘ ZA UWAGĘ

59