Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

IR EXCELLENCE IN RESEARCH

Wydział Informatyki

ZAUFANIE I ZABEZPIECZENIA

dr hab. inż. Jerzy Pejaś, prof. ZUT

Wydział Informatyki

Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie

1

O czym będzie mowa w tym wykładzie?

AGENDA

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

2

Nowe wyzwania bezpieczeństwa

NOWE ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

- Urządzenia komputerowe stają się coraz bardziej rozproszone, bez nadzoru i narażone fizycznie
  - Komputery w Internecie (z niezaufanymi właścicielami)
  - Urządzenia wbudowane (samochody, sprzęt AGD)
  - Urządzenia mobilne (telefony komórkowe, urządzenia PDA, laptopy)
  - Stacje bazowe i bezprzewodowe punkty dostępowe
- Atakujący mogą fizycznie manipulować przy urządzeniach
  - Inwazyjne sondowanie
  - Nieinwazyjny pomiar
  - Instalowanie złośliwego oprogramowania

Ataki

ATAKI

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

- Ataki z wykorzystaniem tylko oprogramowania
- Ataki z wykorzystaniem sprzętu
- Inne (nieoczekiwane) sposoby

} Formy hybrydowe

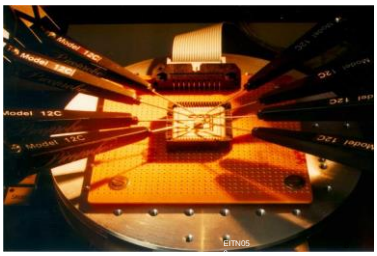
- Przeciwnik może korzystać z narzędzi ataku według własnego wyboru i uznania.
  - Nie można powiedzieć „ten atak jest niedozwolony”
- Ataki są niespodziewane.

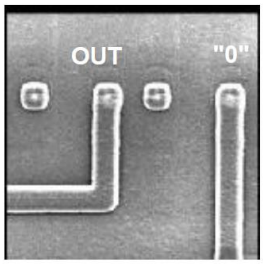
Ataki inwazyjne wykorzystujące sprzęt

ATAKI ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

- **Pasywne**: mikrosondowanie
  - Sonduj magistralę bardzo cienką igłą
  - Odczytaj bezpośrednio dane z magistrali lub z poszczególnych komórek
  - Kilka igieł jednocześnie
- **Aktywne**: modyfikacja obwodu
  - Podłączyć lub rozłączyć mechanizm bezpieczeństwa
    - Odłącz czujniki bezpieczeństwa
    - RNG utknął na stałej wartości
    - Odtworzenie przepalonych bezpieczników
  - Wytnij lub wklej ścieżki za pomocą lasera lub skupionej wiązki jonowej
  - Dodaj elektrody sondy do ukrytych warstw





Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

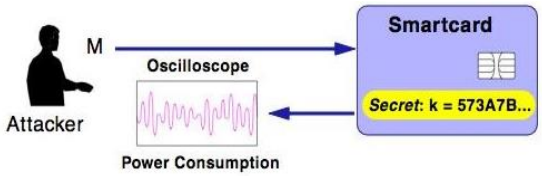
5

Przykład nieoczekiwanego ataku na karty inteligentne

ATAKI ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

- Bezpośrednia obserwacja zużycia prądu przez układ w czasie operacji kryptograficznych
- Ilość pobieranej energii zależy od rodzaju wykonywanych operacji
- Analiza poboru prądu pozwala rozróżnić poszczególne etapy realizacji algorytmu kryptograficznego
- Dokładniejsza analiza pozwala rozróżnić poszczególne operacje



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

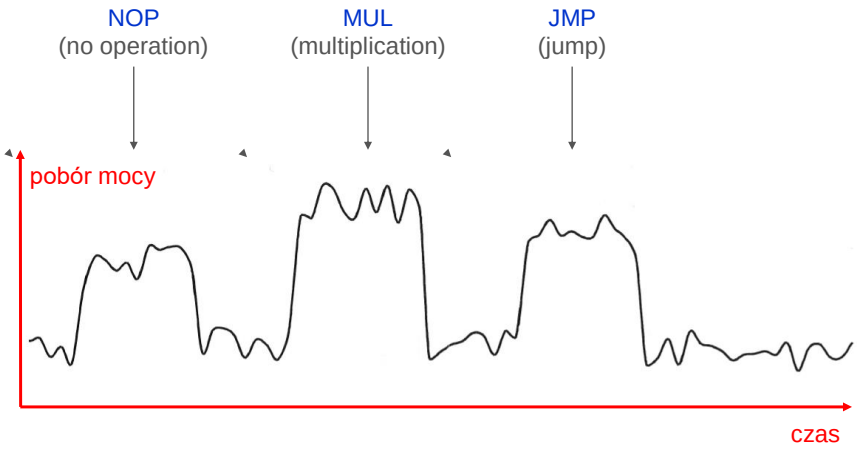
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

6

Przykład nieoczekiwanego ataku na karty inteligentne – analiza czasowa i poboru mocy

ATAKI ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu



Źródło:: Rankl and Effing, "Handbuch der Chipkarten", 2008

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

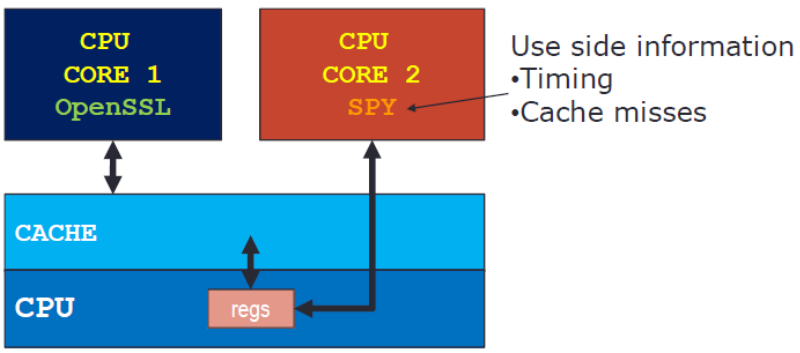
Wydział Informatyki

Ataki kanałami bocznymi - przykład w procesora wielordzeniowego

ATAKI ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Proces SPY “wyłuskuje” klucz z programu wspieranego przez OpenSSL



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

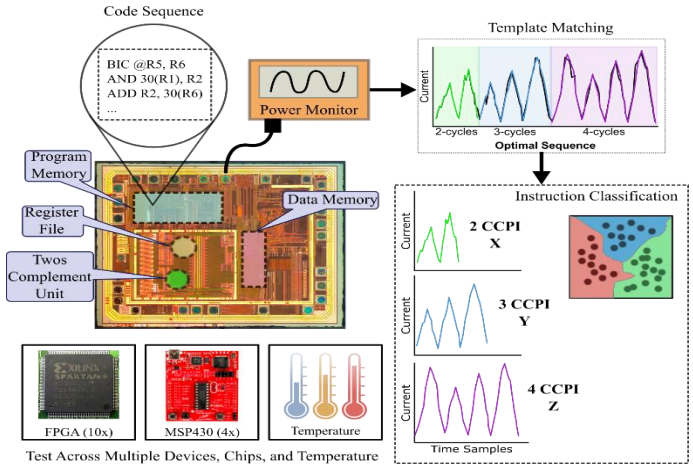
Wydział Informatyki

Ataki kanałami bocznymi – postawienie problemu

ATAKI ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Wykrycie sekwencji wielu instrukcji cyklu zegara, uruchomionych na mikroprocesorze potokowym za pomocą analizy poboru mocy.



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zaufanie – wielki problem

ZAUFANIE ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

- Zaufanie w rozproszonych systemach IT
  - Zaangażowane różne strony o potencjalnie sprzecznych wymaganiach
  - Metody kryptograficzne nie zawsze są przydatne
- Wyzwania
  - Jak zdefiniować zaufanie?
  - Jak określić/weryfikować zaufanie?
  - Jak znane platformy informatyczne mogłyby obsługiwać taką funkcjonalność?
    - Nawet bezpieczny OS nie jest w stanie zweryfikować swojej integralności
- Rola zaufanych obliczeń (ang. trusted computing)
  - Pozwala na wnioskowanie o “wiarygodności” własnej i innych systemów IT

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zaufanie – pojęcia

ZAUFANIE ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zaufanie to:

- przeświadczenie ufającego, że powiernik zachowa się zgodnie z oczekiwaniami, np. dostarczy prawdziwą informację,
- wiara w to przeświadczenie, tj. ufający wierzy, że oczekiwane zachowanie wystąpi, i
- gotowość do podejmowania ryzyka wynikającego z tej wiary w kontekście oczekiwanego konkretnego zachowania się powiernika.

Dwa typy zaufania:

- **zaufanie do wyników** (ang. trust in performance) – zaufanie do tego co wytworzy powiernik; np. oznacza to, że jeśli twórcą wiadomości jest powiernik, to w określonym kontekście ufający uważa ją za wiarygodną;
- **zaufanie wynikające z wiary** (ang. trust in belief) – zaufanie do tego w co wierzy powiernik, np. jeśli powiernik wierzy konkretnej wiadomości, to w określonym kontekście za wiarygodną uważa ją także ufający.

Zaufanie – pojęcia (c.d.)

ZAUFANIE ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Określenia (próba)

1. **Bezpieczny** (ang. secure) system lub komponent nie zawiedzie w odniesieniu do celów ochrony (działa zgodnie z celami polityki bezpieczeństwa)
2. **Zaufany** (ang. trusted): system lub komponent, którego awaria może przełamać cele polityki bezpieczeństwa (Trusted Computing Base, TCB)
3. **Wiarygodny** (ang. trustworthy): stopień, w jakim zachowanie komponentu lub systemu jest wyraźnie zgodne z deklarowaną funkcjonalnością.

Trusted Computing Group (TCG) definiuje system jako zaufany jeśli:

- w zależności od przeznaczenia zawsze zachowuje się zgodnie z oczekiwaniami.

Zaufanie jako przewidywalne zachowanie

ZAUFANIE ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

- Zaufanie to przekonanie, że osoba lub system będzie zachowywał się przewidywalnie, nawet w warunkach stresu
  - Bazuje się na doświadczeniu i/lub poświadczeniach
  - Bazuje się na podstawowych właściwościach (tożsamość, integralność)
  - Łatwo jest je stracić i trudno odzyskać.
- Zaufany system jest ...
  - przewidywalny, nawet w warunkach stresu
  - zaufany ze względu na doświadczenie użytkowników i/lub dostępne dowody
  - bazuje na podstawowych właściwościach (tożsamość, integralność)

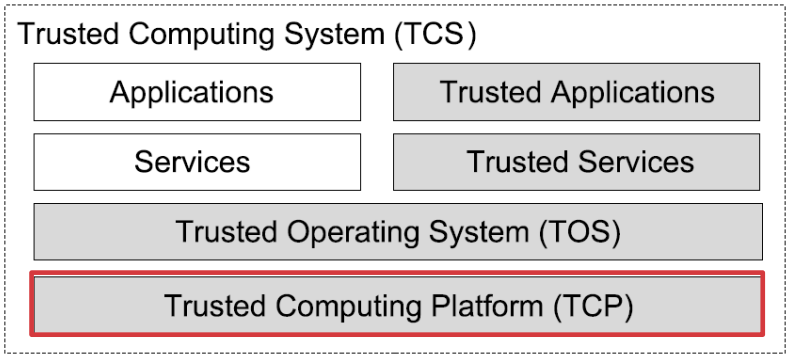
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Trusted Computing System (TCS)

OBLICZENIA ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Trusted Computing System (TCS), c.d.

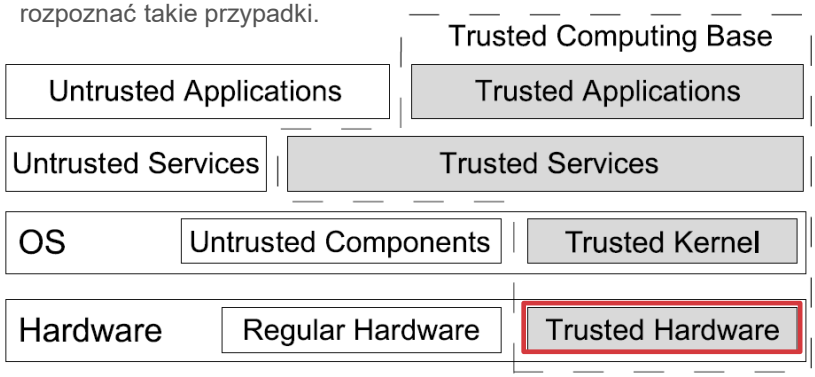
- Zasadniczo Trusted Computing Platform obejmuje rozszerzenia sprzętowe systemu, które są niezbędne do wdrożenia idei zaufanego komputera.
  - Rozszerzenia te obejmują zarówno dodawanie nowych komponentów do płyty głównej systemu oraz odpowiedniego oprogramowania układowego w celu obsługi nowych komponentów (przykład: Trusted Platform Module wg TCG)
- Nie ma jednoznacznej definicji zaufanego systemu operacyjnego (Trusted-OS).
  - Zaufany system operacyjny można ogólnie rozumieć jako połączenie bezpiecznego jądra systemu operacyjnego (zaufanego jądra) oraz wiarygodnych usług i aplikacji.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Trusted Computing Base (TCB)

- Trusted Computing Base (TCB) stanowi rdzeń Trusted Computing System.
  - Zawiera wszystkie elementy, których integralność ma kluczowe znaczenie dla wiarygodności systemu. Stąd należy uniemożliwić kompromitację jakiegokolwiek z tych komponentów lub przynajmniej rozpoznać takie przypadki.



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Podstawowa idea zaufanych obliczeń

IDEA ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

- Używać specjalistycznego sprzętu zabezpieczającego jako części TCB w systemie komputerowym. Dzięki temu system:
  - nie powinien być narażony na oddziaływanie szkodliwgo oprogramowania
  - może zweryfikować integralność jądra systemu operacyjnego
  - może utrudniać fizyczną manipulację
  - może zgłaszać status systemu zdalnym podmiotom
  - może zgłaszać tożsamość systemu zdalnym podmiotom
- Dzięki specjalistycznemu sprzętowi można osiągnąć wyższy poziom zaufania do tego, że system będzie działał zgodnie oczekiwaniami/specyfikacjami.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

17

Dwie kluczowe cechy zaufanych obliczeń

CECHY ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

- **Opieczętowany magazyn danych (ang. Sealed Data Storage)**
  - przechowywane dane można otworzyć tylko za pomocą właściwej kombinacji oprogramowanie/sprzętu;
  - magazyn może być używany do zarządzania prawami autorskimi (Digital Rights Management, DRM).
- **Zdalna atestacja (ang. Remote Attestation)** - zdalna certyfikacja mająca na celu potwierdzenie, że w systemie działa tylko autoryzowany kod.

- **Obawy.** Utrata prywatności przez użytkowników końcowych.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

18

ZAUFANIE A OBLICZENIA ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Czym jest „zaufanie” w kontekście zaufanych obliczeń?

- Mieć zaufanie do założeń dotyczących bezpieczeństwa
- Zaufanie oznacza wiarę w to, że przyjęte asercje bezpieczeństwa są spełnione

  „Zaufany komponent, operacja lub proces to takie elementy, których zachowanie uważa się prawidłowe w każdych warunkach operacyjnych, i w przypadku których zakłada się, że są odporne na szkodliwe oprogramowanie, wirusy i manipulacje.”
- Zaufany komponent tak długo egzekwuje zasady bezpieczeństwa, jak długo te założenia są spełnione
- Zaufany komponent narusza zasady bezpieczeństwa, jeśli zostanie przełamany (np. zepsuje się)
- Pytanie: zaufany przez kogo i w realizacji czego?
  - Zaufany przez użytkownika, dostawcę lub podmiot zewnętrzny (ABW, CBA)
  - Co jeśli mają sprzeczne interesy?

WZMOCNIENIE ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

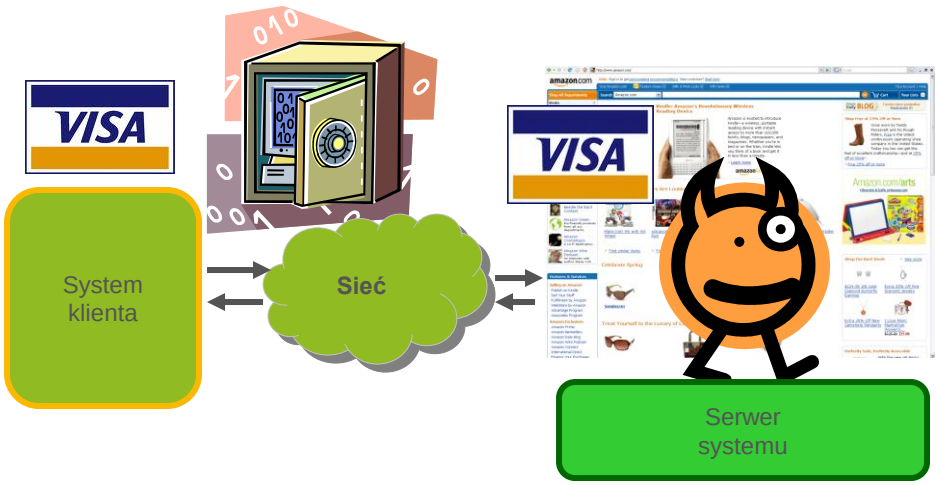
Podejścia do wzmocnienia bezpieczeństwa platformy

- Wzmocniony system operacyjny
  - SE (Security Enhanced) Linux, Trusted Solaris, Windows 7/8/10/11
- Dodatkowe funkcje bezpieczeństwa procesora
  - Warstwy ochronne, NoExecute, ASLR (Address Space Layout Randomization)
- Technologie wirtualizacji
  - Separacja procesów poprzez separpwanie systemów wirtualnych
- Zaufane obliczenia
  - Dodanie bezpiecznego sprzętu do platformy obliczeniowej
  - Na przykład TPM (moduł zaufanej platformy)
- Bazowanie na bezpiecznym sprzęcie zewnętrznym względem platformy obliczeniowej
  - Karty inteligentne
  - Tokeny sprzętowe

Potrzeba zaufania w systemach – uzasadnienie

UZASADNIENIE ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

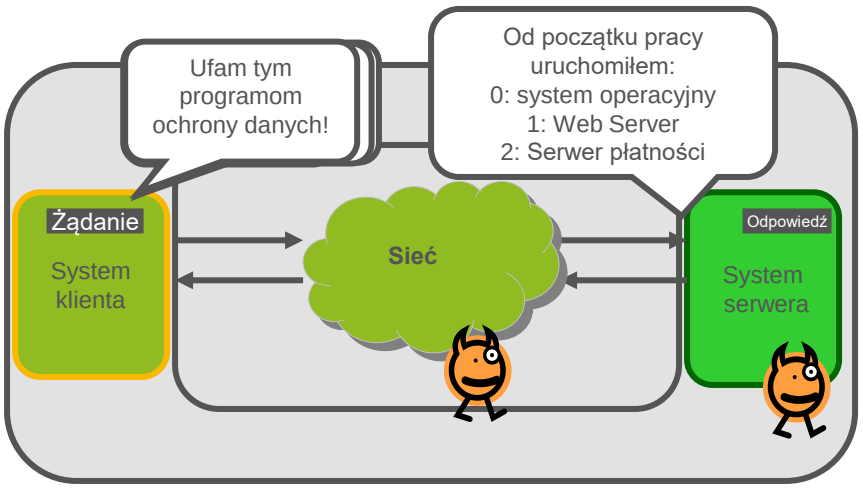


Jak zaufać zdalnemu serwerowi?

Potrzeba zaufania w systemach – idea

IDEA ...

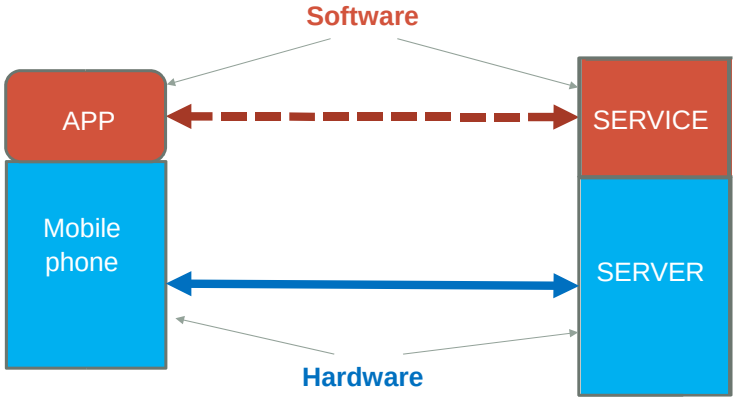
- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu



Jak zaufać (zdalnej) usłudze?

ZDALNA USŁUGA ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu



Czy podział na SW i HW jest istotny?

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

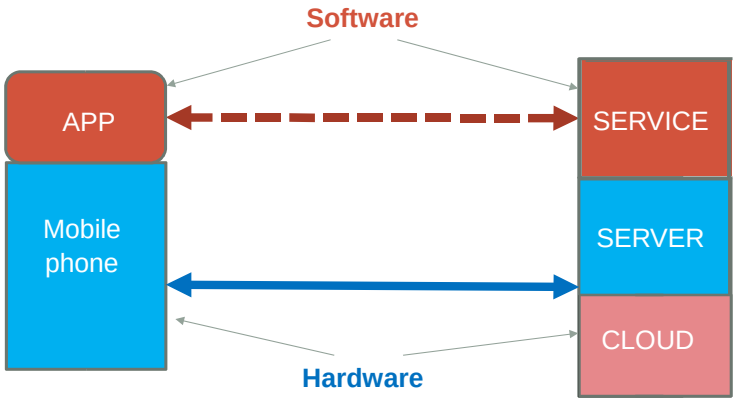
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

23

A jak zaufać usłudze w chmurze?

ZAUFANIE A CHMURA

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

24

Od zaufanych obliczeń do zaufanej platformy?

ZAUFANA PLATFORMA ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

- Zaufane obliczenia
  - Wymagają zaufania do oprogramowania (aplikacji)

Zaufane, bezpieczne oprogramowanie nie jest przedmiotem tego wykładu

SERVICE

- Wymagają zaufania do systemu bazowego

Zaufana platforma

SERVER

CLOUD SERVER

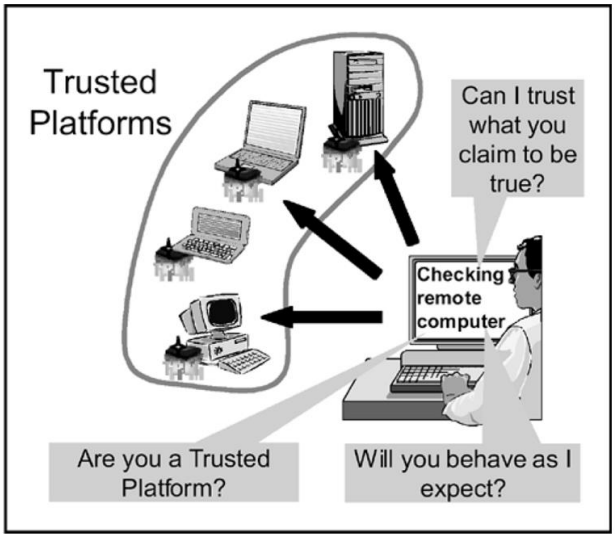
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Potrzeba zaufania w rzeczywistych systemach IT

SYSTEMY IT ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zalety zaufanej platformy

ZALETY ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Gdy platforma może udowodnić, że uruchamia oczekiwany plik wykonywalny, to w przypadku:

- obliczeń w systemach stron trzecich (np. systemy chmurowe)
  - ... otrzymujemy poprawne wyniki
- wspierania polityki „przynieś swoje własne urządzenie” (Bring Your Own Device, BYOD)
  - dane różnych interesariuszy są bezpiecznie przechowywane na urządzeniu
- płatności elektronicznych
  - prawidłowa kwota, anonimowy (do pewnego stopnia) zaufany interfejs użytkownika
- cyfrowego zarządzanie prawami (Digital Rights Management, DRM)
  - egzekwowane są prawa autorskie do treści (muzyki, wideo, programów itp.)
- czujników i nadzoru
  - można polegać na otrzymanych danych
- i tak dalej ...

Intuicyjne modele zaufanych platform

MODELE ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

- Platforma otwarta
  (np. PC, PDA, iOS, Android, urządzenie Linux)
  - Platforma obliczeniowa ogólnego przeznaczenia

Można dodawać/modyfikować oprogramowanie

- Platforma zamknięta
  (np. bankomat, przystawka STB (Set-top box), konsola do gier, odbiornik satelitarny, większość starszych telefonów (wcześniej iOS, Android))
  - Specjalistyczne urządzenie komputerowe

Potrafi się bronić przed zagrożeniami

Wiemy, co jest w środku

MODELE ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Intuicyjne modele zaufanych platform (c.d.)

Zaufane obliczenia łączą w sobie najlepsze właściwości obu platform

- **Platforma otwarta**: zezwala aplikacjom pochodzącym z wielu różnych źródeł na działanie na tej samej platformie
- **Platforma zamknięta**:
  - Pozwala wykonać tylko „znane" oprogramowanie
  - Izoluje komponenty oprogramowania w celu ograniczenia rozprzestrzeniania się złośliwego kodu
  - Zdalne podmioty mogą ustalić, które oprogramowanie jest uruchomione i czy mogą oczekiwać, że platforma będzie zachowywała się zgodnie z oczekiwaniami

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANY A GODNY ZAUFANIA ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Zaufany (ang. trusted) a wiarygodny (ang. trustworthy)

Po co rozróżniamy zaufaną i wiarygodną (godną zaufania) platformę?

Zaufany. Systemowi można zaufać, ale czy jest on wiarygodny?

Wiarygodny. System może spełnić wymagania określone przez metodologię. Czy metodologia jest zatem wiarygodna (... i otrzymujemy rekurencję), czy po prostu ufamy tej metodologii?

Komentarz. System po uzyskaniu pozytywnej oceny na poziomie EALx wykonanej zgodnie z metodologią Common Criteria (norma ISO 15408) jest wiarygodny.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

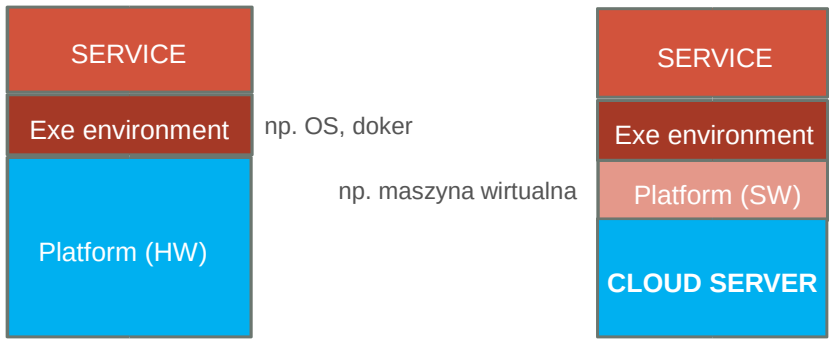
Wydział Informatyki

Jak uzyskać wiarygodność?

GODNY ZAUFANIA ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Jak radzić sobie z różnicami?



Realizacja tradycyjna | Realizacja chmurowa

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie | Wydział Informatyki

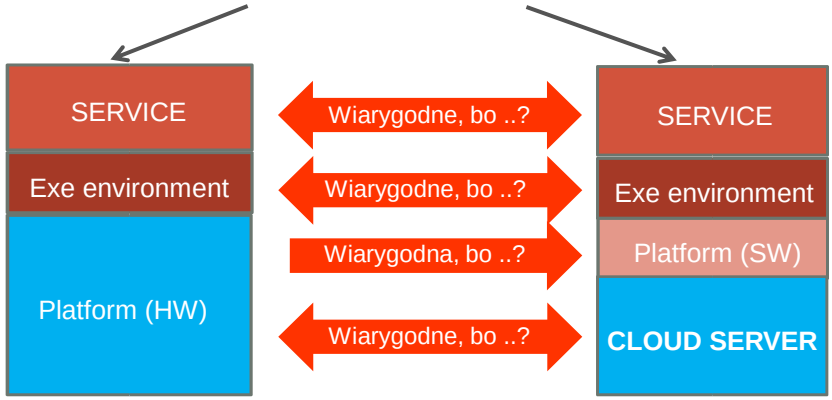
31

Jak uzyskać wiarygodność?

GODNY ZAUFANIA ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Jak radzić sobie z różnicami między rozwiązaniem chmurowym a tradycyjnym?



Realizacja tradycyjna | Realizacja chmurowa

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie | Wydział Informatyki

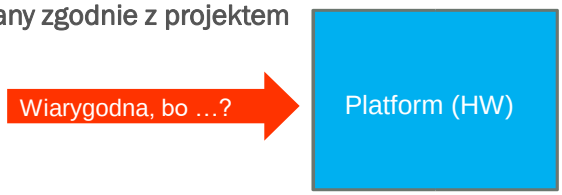
32

SPRZĘT A ZAUFANIE ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Jak i dlaczego ufać sprzętowi?

- Zaufanie dzięki reputacji
- Zaufanie dzięki trzeciej stronie
- Uzasadnione zaufanie do projektu
  - Przeglądy
  - Dowody (poprzez modelowanie sprzętu)
- Uzasadnione zaufanie do wytwarzania produktu
  - Sprzęt jest produkowany zgodnie z projektem



ZAUFANA INFRASTRUKTURA OBLICZENIOWA

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

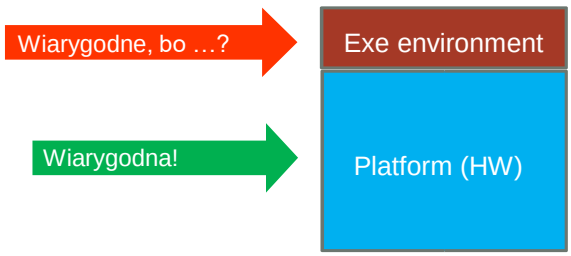
33

ŚRODOWISKO WYKONANIA ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Jak i dlaczego ufać środowisku wykonywania?

- Zaufanie dzięki reputacji
- Ponieważ sprawdziliśmy kod i sami tam go umieściliśmy.
- Ponieważ sprzęt rozpocznie wykonywanie tylko tego kodu, który zatwierdziliśmy (i sprawdziliśmy, czy jest OK)



ZAUFANA INFRASTRUKTURA OBLICZENIOWA

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

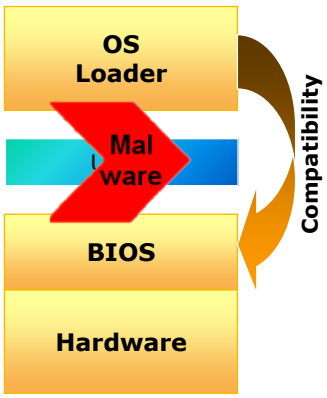
34

Przykład: uruchamianie systemu z użyciem UEFI? (Unified (EFI)/Extensible Firmware Interface (EFI)

UEFI ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

- UEFI to specyfikacja interfejsu
- Oddzielenie BIOS-u od systemu operacyjnego
  - Odseparowanie rozwoju obu komponentów
- Kompatybilny z założenia
  - Ewolucja, nie rewolucja
- Modułowy i rozszerzalny
  - Wartość dodana neutralna dla systemu operacyjnego
- Zapewnienie wydajnych opcji wymiany pamięci ROM
  - Wspólne źródło dla wielu architektur CPU
- Dopełnia istniejące interfejsy



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

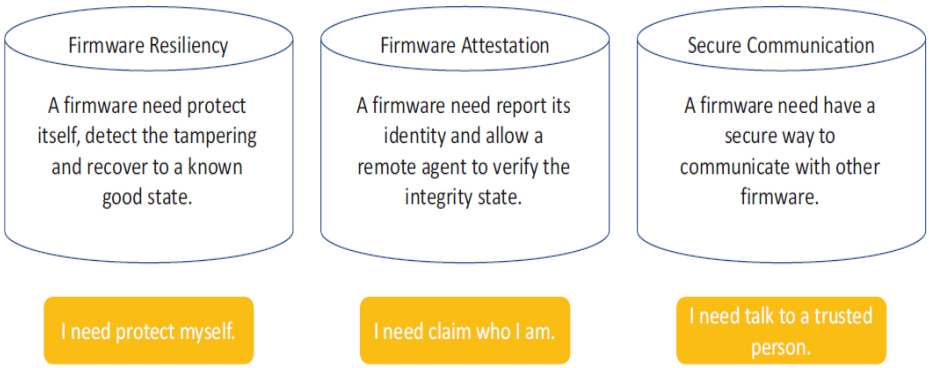
Wydział Informatyki

Bezpieczeństwo oprogramowania przysprzętowego (ang. firmware security)

UEFI ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu

Oprogramowanie przysprzętowe jest podstawą bezpieczeństwa systemu komputerowego.



J. Yao, V. Zimmer *Building Secure Firmware - Armoring the Foundation of the Platform*. Apress 2020

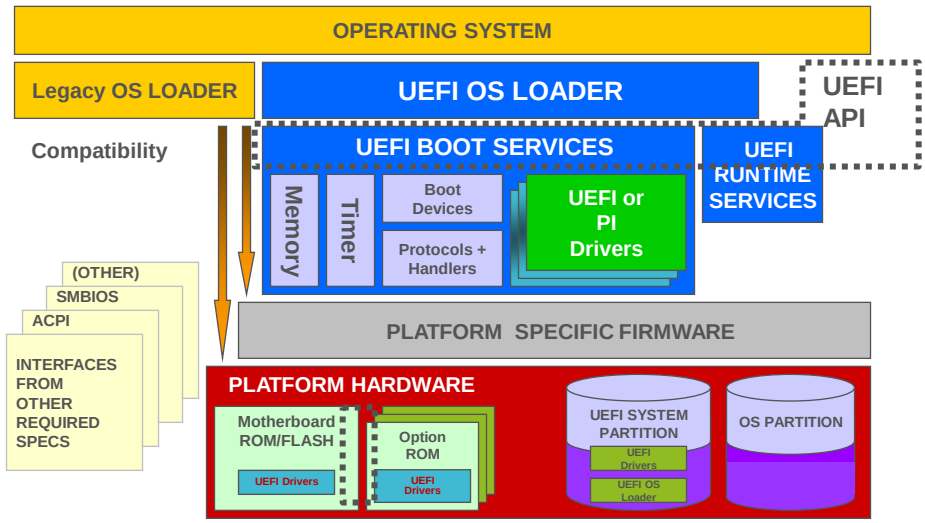
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Co to jest UEFI? (Unified (EFI)/Extensible Firmware Interface (EFI)

UEFI ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

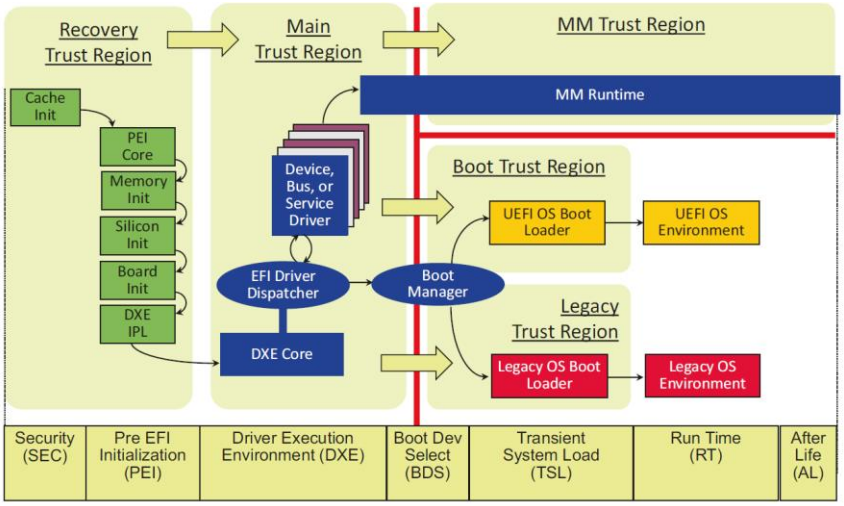
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

37

Proces uruchamiania systemu komputerowego z UEFI

UEFI ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu



J. Yao, V. Zimmer *Building Secure Firmware - Armoring the Foundation of the Platform*. Apress 2020

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

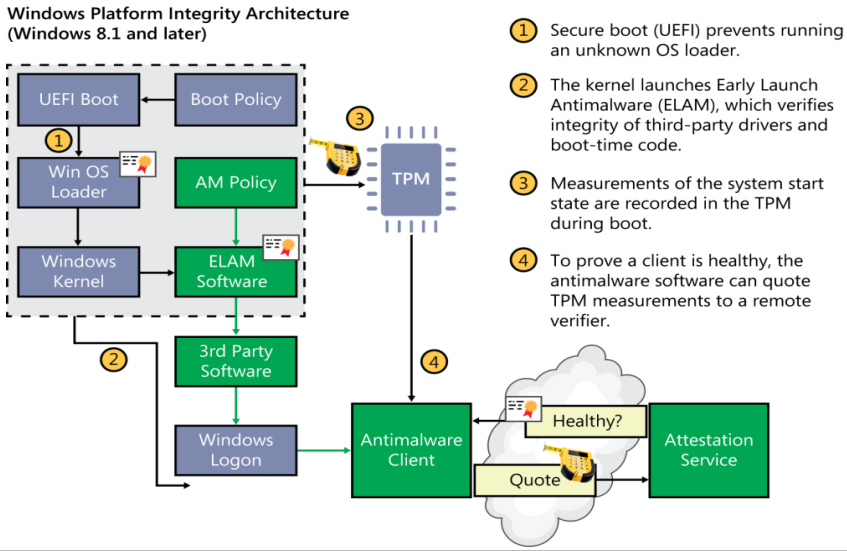
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

38

Przykład - zabezpieczenie procesu rozruchu (Windows)

BEZPIECZNY ROZRUCH ...

- Wyzwania bezpieczeństwa
- Zaufanie jako przewidywalne zachowanie
- Rola elementów zaufanej infrastruktury
- Zaufane obliczenia a zaufana platforma
- Modele zaufanych platform - wady, zalety
- Zaufanie do sprzętu



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

39

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

IIR EXCELLENCE IN RESEARCH

DZIĘKUJĘ ZA UWAGĘ

Wydział Informatyki

40