Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

IR EXCELLENCE IN RESEARCH

Wydział Informatyki

GŁÓWNE ŹRÓDŁA ZAUFANIA DO OBLICZEŃ

dr hab. inż. Jerzy Pejaś, prof. ZUT

Wydział Informatyki

Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie

1

AGENDA

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

O czym będzie mowa w tym wykładzie?

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

Podstawowa idea zaufanej platformy

IDEA ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Sprzętowe i programowe zaufane komponenty
- Oferuje szereg funkcji zaufanych
  - W szczególności zestaw funkcji kryptograficznych i funkcji bezpieczeństwa
- Tworzy idealną bazę do budowania zaufania do oprogramowania
- Zapewnia sprzętową ochronę danych wrażliwych
  - np. kluczy, liczników
- Pożądane cele praktyczne
  - Trusted Computing Base (TCB) powinna być minimalizowana
  - Kompatybilność z systemami źródłowymi

Conventional Platform | Trusted Platform

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie | Wydział Informatyki

Łańcuch zaufania

ŁAŃCUCH ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

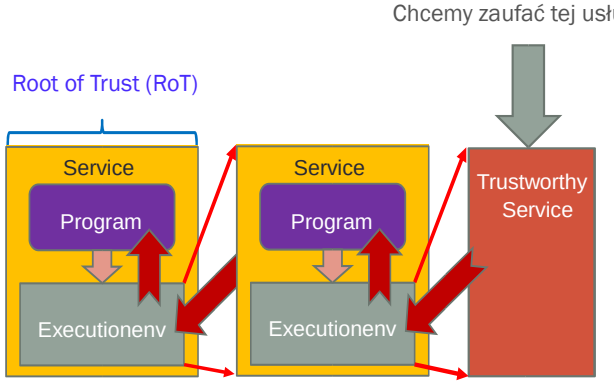
- Rozważmy jednostki (ang. entities) $\boldsymbol{E_0}$, ... , $\boldsymbol{E_n}$
- Celem jest uzyskanie zaufania do jednostki $\boldsymbol{E_n}$
  - Z punktu widzenia wykonywanych operacji: $\boldsymbol{E_0}$ wywołuje $\boldsymbol{E_1}$, $\boldsymbol{E_1}$ wywołuje $\boldsymbol{E_2}$, itd.
  - Aby ufać $\boldsymbol{E_n}$ należy ufać $\boldsymbol{E_{n-1}}$
  - Sekwencja $\boldsymbol{E_0}$, $\boldsymbol{E_1}$ to $\boldsymbol{E_n}$ tworzy „łańcuch zaufania” (ścieżkę zaufania)
- Zaufanie przechodnie (tranzytywne) od $\boldsymbol{E_0}$ do $\boldsymbol{E_1}$ do $\boldsymbol{E_2}$, itd.
  - Zaufanie E_2 wymaga zaufania do E_0 i E_1
  - Jednak: zaufanie do E_0 nie implikuje zaufania do E_2

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie | Wydział Informatyki

Zaufane obliczenia: początek łańcucha zaufania - główny punkt zaufania (ang. Root of Trust, RoT)

ROT ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



Rekurencja musi kończyć się na komponencie, któremu możemy zaufać, na przykład układowi sprzętowemu firmy Intel TXT (**Intel® Trusted Execution Technology**).

Uwaga: RoT to nie tylko dane (np. klucze), ale także logika. Dlatego mówimy, że RoT to silnik.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

5

Główny punkt zaufania (ang. Root of Trust)

ROT ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- RoT (Root of Trust) jest tą częścią systemu, którą uważamy za wiarygodną.
- Dlaczego dana część systemu może być wiarygodna?
  - Bo przeprowadziliśmy bardzo staranne analizy projektu i wdrożenia
    - Na przykład w oparciu o metodologię Common Criteria (wg ISO 15408)
  - Bo możemy zweryfikować, czy ktoś inny (trzecia strona) uważa tę część systemu za godną zaufania
    - Poświadczenie o zgodności, certyfikat (np. wydany zgodnie ze specyfikacją FIPS 140-2)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

6

Różne główne punkty zaufania (ang. Roots of Trust)

INFORMACJE ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Warto przyjąć, że RoT składa się z różnych typów RoT, z których każdy specjalizuje się w realizacji innych zadań.
- **Główne źródło zaufania do pomiaru** (ang. Root of Trust for Measurement, RTM)
  - Silnik obliczeniowy zdolny do wykonywania wiarygodnych pomiarów integralności (tzw. **metryk** integralności).
- **Główne źródło zaufania do magazynu** (ang. Root of Trust for Storage, RTS)
  - Silnik obliczeniowy, który chroni użycie i dostęp do danych/kluczy
- **Główne źródło zaufania do raportów** (ang. Root of Trust for Reporting, RTR)
  - Silnik obliczeniowy zdolny do niezawodnego raportowania informacji będących w posiadaniu RTS (tzw. **atestacja** komponentu)

Pożądane prymitywy (własności pierwotne)

PRYMITYWY ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Metryki na potrzeby konfiguracji kodu oraz tożsamości
  - Zachowanie się operacji I /O hosta zależy od stanu początkowego
  - Przykład prostej metryki: wartość skrótu z kodu binarnego
  - Problematyczne wtedy, gdy funkcjonalność kodu zależy od innego kodu nieuwzględnionego w skrócie (np. wspólne lub dynamicznie łączone biblioteki)
- Weryfikacja integralności (**atestacja**)
  - Umożliwia platformie obliczeniowej eksportowanie weryfikowalnych informacji o jej właściwościach (np. tożsamości i stanie początkowym)
  - Wynika z wymogu uzasadnia zaufania do kodu wykonywalnego oraz środowiska aplikacji znajdującej się na zdalnej platformie obliczeniowej

Pożądane prymitywy (własności pierwotne)

PRYMITYWY …

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- **Bezpieczny magazyn**
  - Bezpieczne przechowywanie danych na tradycyjnych niezaufanych nośnikach (np. twarde dyski)
  - Szyfrowanie danych i zapewnienie, że nikt inny nie może ich odszyfrować
- **Silna izolacja procesów**
  - Zapewnienie separacji procesów (przestrzeni pamięci)
  - Uniemożliwienie procesowi odczytu lub modyfikowania pamięci innego procesu
- **Bezpieczne operacje I/O**
  - Pozwala aplikacjom zbudować zaufanie do końcowych operacji wejścia i wyjścia
  - Gwarantuje użytkownikowi, że bezpiecznie współdziała z właściwymi aplikacjami

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

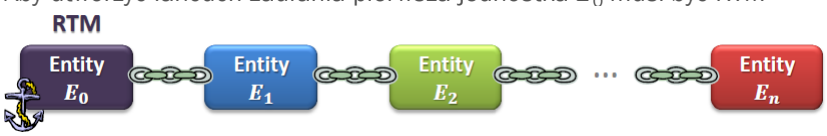
9

Łańcuch pomiarów

ŁAŃCUCH …

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Co jest konieczne do zaufania łańcuchowi pomiarów?
  - Tożsamość każdej jednostki E_i należącej do łańcucha
  - **Tożsamość** = pomiar metryki (zgodnie z definicją TCG)
    - Na przykład skrót z kodu binarnego E_i
  - Ogólny przepływ: każda jednostka E_i mierzy swojego następcę E_{i+1} przed przekazaniem do niego kontroli
- Kto mierzy E_0?
- Główny punkt zaufania do pomiarów (RTM, ang. Root of Trust for Measurements)
  - Musi być zaufany, brak mechanizmu pomiaru E_0
  - Aby utworzyć łańcuch zaufania pierwsza jednostka E_0 musi być RTM



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

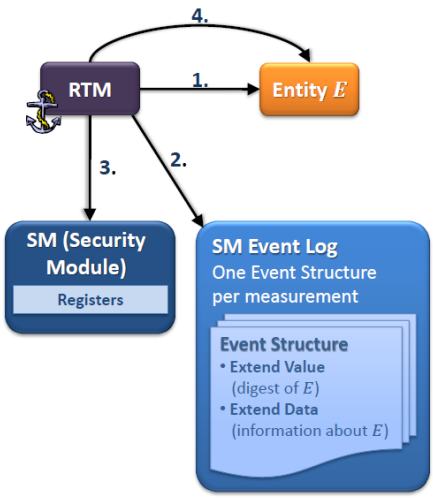
10

Wykonywanie pomiarów integralności

POMIAR ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

1. RTM mierzy jednostkę E
2. RTM tworzy Event Structure w SM Event Log
   - SM Event Log zawiera Event Structures dla wszystkich pomiarów, o które poszerzony jest SM
   - SM Event Log może być przechowywany na dowolnym (niezaufanym) nośniku (np. na twardym dysku)
3. RTM rozszerza pomiary wartości w rejestrach SM
4. RTM przekazuje kontrolę do jednostki E



Source: Prof. Dr.-Ing. Ahmad-Reza Sadeghi, Ruhr University Bochum

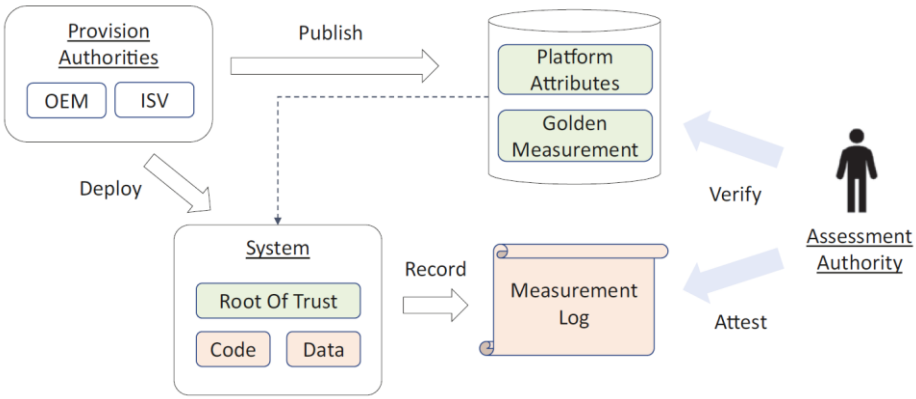
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Przykład pomiaru i atestacji oprogramowania sprzętowego

ŁAŃCUCH ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



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

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

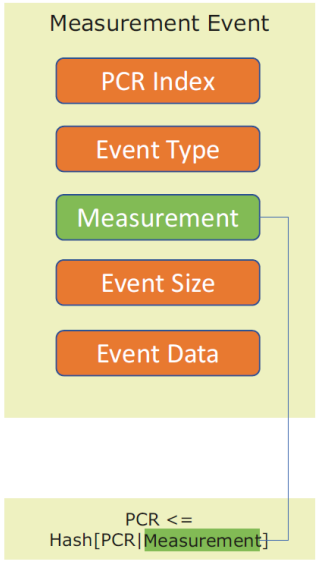
Wydział Informatyki

Przykład Event Structure w SM Event Log

LOGI ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

```
//Structure to be added to the Event Log
typedef struct {
  //PCRIndex event extended PCR
  TCG_PCRINDEX PCRIndex;
  TCG_EVENTTYPE EventType;
  //Value extended into PCRIndex
  TCG_DIGEST Digest;
  //Size of the event data
  UINT32 EventSize;
  //The event data
  UINT8 Event[1];
} TCG_PCR_EVENT;
```



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

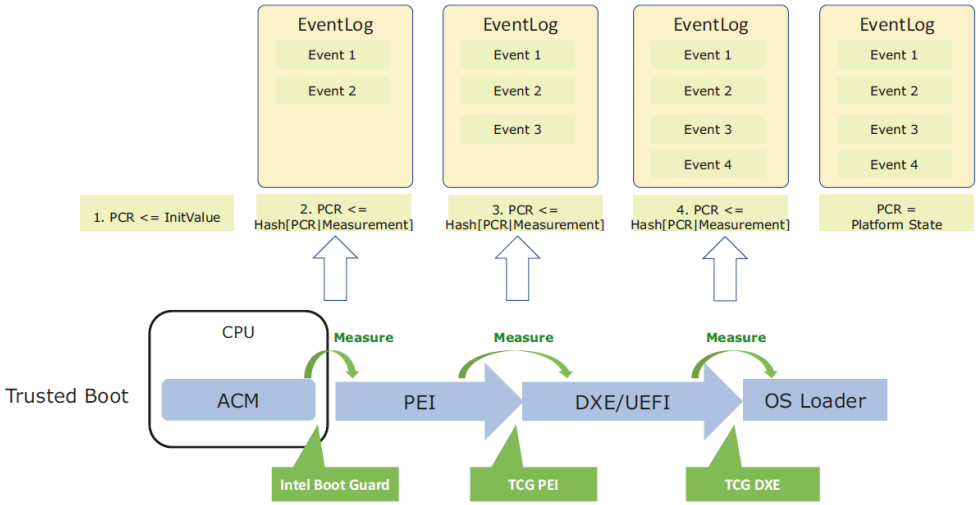
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zapisywanie dziennika zdarzeń pomiarów TPM podczas uruchamiania systemu

LOGI ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



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

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Zaufane środowisko wykonawcze (ang. Trusted Execution Environment, TEE)

SPECYFIKACJE ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

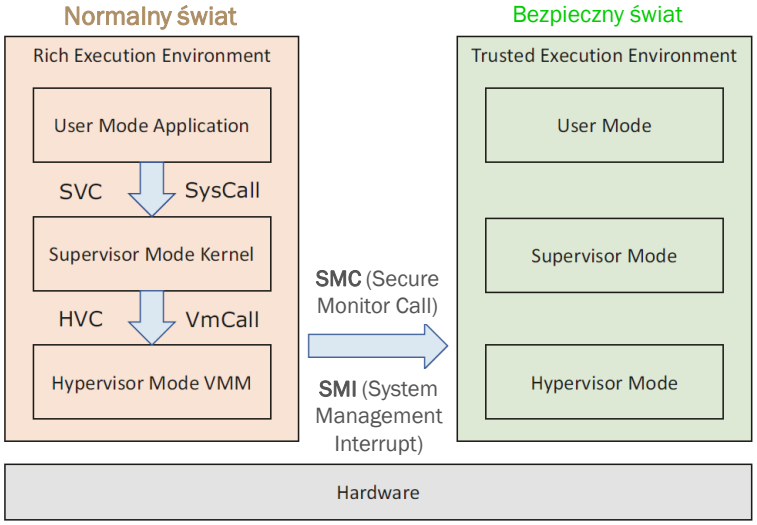
- Zaufane środowisko wykonawcze (TEE) oznacza bezpieczny obszar, który może zagwarantować poufność i integralność kodu i danych znajdujących się w tym obszarze.
- Zazwyczaj TEE jest odizolowanym środowiskiem wykonawczym.
- Może być zaimplementowane jako specjalny bezpieczny tryb pracy procesora głównego (tzw. CPU-based TEE), lub TEE może być utrzymywane za pomocą bezpiecznego koprocesora (ang. Cooprocesor-based TEE).
- Przykłady:
  - CPU-based TEE: ARM TrustZone, Intel SGX, AMD SEV, RISC-V/ARM-M MultiZone,
  - Cooprocesor-based TEE: Intel Converged Security and Management Engine (CSME), Google Titan, TPM.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

CPU-based TEE - architektura

SPECYFIKACJE ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



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

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

Czy zaufane środowisko wykonawcze jest zawsze bezpieczne?

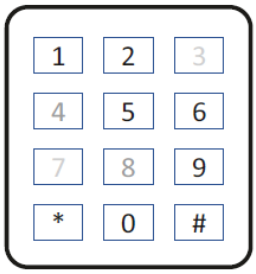
SPECYFIKACJE ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

Niestety, ale nie!

Najgroźniejsze są ataki typu **Side Channel** (ataki z wykorzystaniem kanału bocznego) - **ataki programowe** (np. atak czasowy i ataki na pamięć podręczną) i **ataki sprzętowe** (np. analiza poboru mocy).

Przykład: zużyta klawiatura numeryczna.



Na podstawie widocznej obok klawiatury można wywnioskować, że klawisze 3 i 7 są mocno zużyte, zaś 4 i 8 lekko zużyte. W skład kodu dostępu wchodzą wiec cztery cyfry: 3, 4, 7 i 8.
Co więcej, większe zużycie klawiszy 3 i 7 sugeruje, że cyfry 3 i 7 powtarzają się w kodzie dostępu.

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

Tradycyjne ataki z wykorzystaniem kanału bocznego
Atak czasowy (ang. Timing Attack)

SPECYFIKACJE ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Przykład: porównanie podanego kodu dostępu z oczekiwanym kodem.

```
bool compare_mem(byte *a, size_t a_len, byte *b,
                                        size_t b_len){
   if (a_len != b_len) { // zależne od danych!
      return false;
   }
   for (size_t i = 0; i < a_len; i++) {
      if (a[i] != b[i]) { // zależne od danych!
         return false;
      }
   }
   return true;
}
```

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

Tradycyjne ataki z wykorzystaniem kanału bocznego
Atak czasowy (ang. Timing Attack)

SPECYFIKACJE ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- **Przykład**: kod dostępu P@ssw0rd.
- **Spostrzeżenie**: czas wykonania funkcji jest proporcjonalny do liczby znaków pasujących w kodzie.

	P	@	s	s	w	0	r	d
Round 1	P	*	*	*	*	*	*	*
Round 2	P	@	*	*	*	*	*	*
Round 3	P	@	s	*	*	*	*	*
Round 4	P	@	s	s	*	*	*	*
Round 5	P	@	s	s	w	*	*	*
Round 6	P	@	s	s	w	0	*	*
Round 7	P	@	s	s	w	0	r	*
Round 8	P	@	s	s	w	0	r	d

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Tradycyjne ataki z wykorzystaniem kanału bocznego
Atak czasowy (ang. Timing Attack)

SPECYFIKACJE ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Wyeliminowanie ataku polega na wptowadzeniu do funkcji takich zmian, aby czas wykonania pętli **for** stał się niezależny od liczby dopasowywanych znaków.

```
bool compare_mem (byte *a, size_t a_len, byte *b,
                                        size_t b_len) {
   volatile size_t x = a_len ^ b_len;

   for (size_t i = 0; ((i < a_len) & (i < b_len)); i++) {
      x |= a[i] ^ b[i];
   }
   return (x==0);
}
```

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

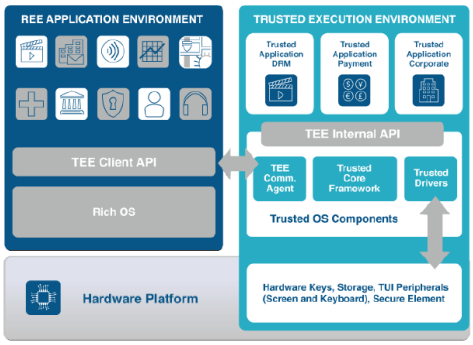
Specyfikacje przemysłowe/wymagania dotyczące RoT

SPECYFIKACJE …

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Trusted Computing Group (TCG) – Trusted Platform Module (TPM)
- ARM TrustZone
- Intel SGX

Trusted Execution Environments (TEE)



- GlobalPlatform
- NIST 800-207 **Zero Trust Architecture**, 2020

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

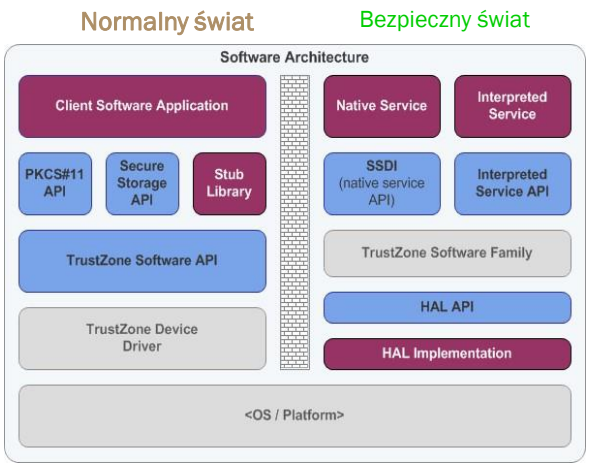
Wydział Informatyki

ARM TrustZone

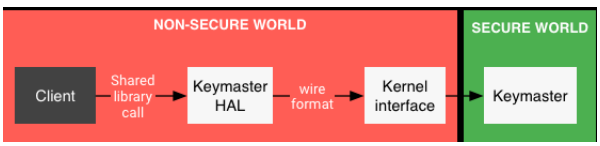
ARM …

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Specjalny tryb pracy procesora ARM



- Dzieli System-On-Chip (SoC) na „normalny świat” i „bezpieczny świat” (inaczej, na “nieza-ufany” i “zaufany”)



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

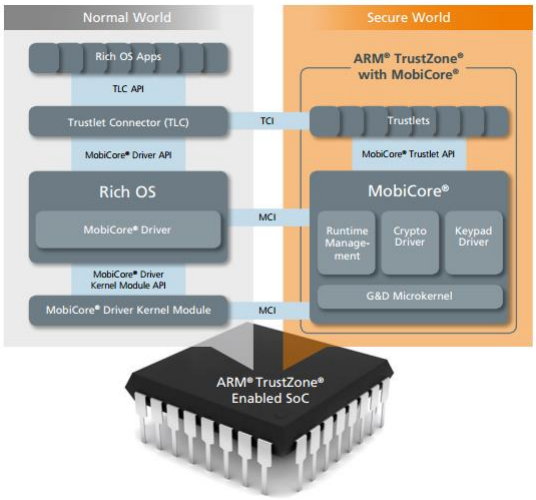
Wydział Informatyki

Podstawowa idea

ARM IDEA ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Zawiera bit **NS** (*Non-secure*), który określa, czy wykonanie programu odbywa się w świecie bezpiecznym, czy też normalnym
  - użyj tego bitu, aby oznaczyć bezpieczne dane w całym systemie
    - szyny (ang. buses)
    - pamięć podręczna
    - strony pamięci
- Monitor
  - zarządza bitem NS
  - zarządza przejściem do i z trybu bezpieczeństwa
  - mały stały interfejs API (pozwala lepiej sprawdzić/zweryfikować kod)
- Trustlet: zaufany proces lub aplikacja



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

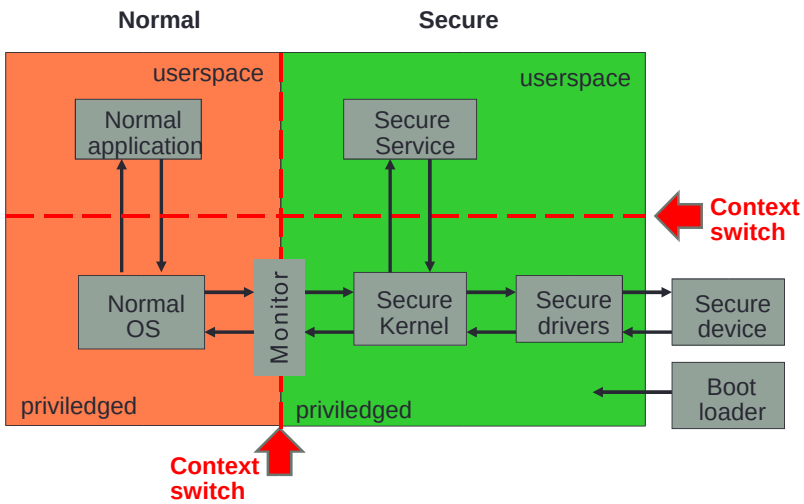
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

23

ARM TrustZone - przełączanie z trybu normalnego w bezpieczny

ARM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

24

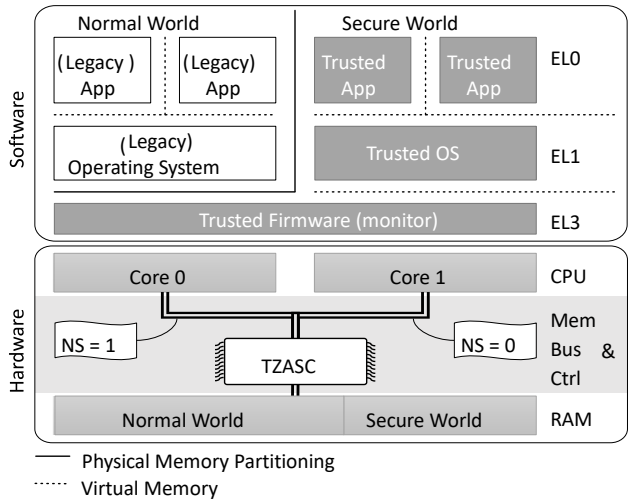
ARM TrustZone - software and hardware components (A-profile)

ARM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- EL3 (monitor mode): runs the ARM Trusted Firmware
- EL1: for the OS kernel
- EL0: for execution of application code.

- Software can be executed in normal world or in secure world.
- Isolation between these two worlds is enforced by the memory controller (TZASC) that checks for each memory access which world it originates from

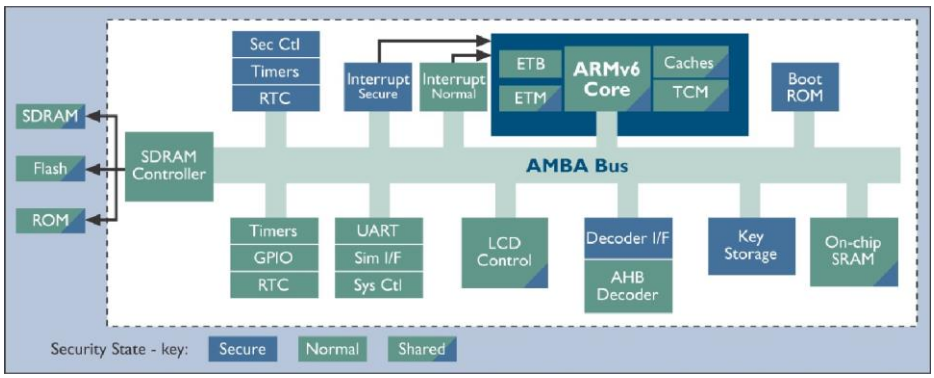


F. Brasser, et. al. "SANCTUARY: ARMing TrustZone with User-space Enclaves", Network and Distributed Systems Security (NDSS), 2019

ARM TrustZone wykorzystuje funkcje sprzętowe - przykładowy system

ARM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



ARM TrustZone jest wykorzystywany w wielu smartfonach z systemem Android

Korzystanie z ARM TrustZone

ARM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

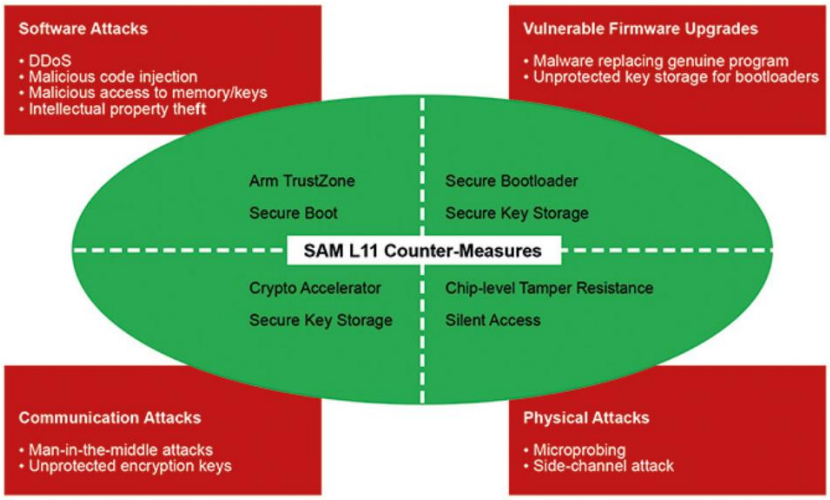
- Powszechnie stosowany w smartfonach z chipsetami Qualcomm i Samsung
- Stanowi rdzeń rozwiązania KNOX firmy Samsung

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Wydział Informatyki

ARM TrustZone – ochrona przed różnymi rodzajami ataków

ARM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



Note: Side channel attack referred here is data remanence

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Wydział Informatyki

Intel Software Guard eXtensions (SGX)

SGX ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- SGX w nowej technologii wprowadzonej w chipsetach Intela
- Architektura SGX zawiera 17 nowych instrukcji, nowe struktury procesorów i nowy tryb wykonywania (dodatkowe rozszerzenia dla serwerów).
- Architektura SGX obejmuje ładowanie enklawy do chronionej pamięci, dostęp do zasobów poprzez odwzorowania tabel stron i planowanie wykonanie aplikacji obsługującej enklawę.
  - Stąd system oprogramowanie ciągle utrzymuje kontrolę nad tym, do których zasobów ma dostęp enklawa.
- Aplikacja może być hermetyzowana przez pojedynczą enklawę lub może być rozkładana na mniejsze komponenty w taki sposób, że w enklawie umieszczane są tylko enklawy krytyczne.

Enklawy w SGX

SGX ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Enklawy to izolowane regiony pamięci kodu i danych
- Jedna część pamięci fizycznej (RAM) jest zarezerwowana dla enklaw i nosi nazwę Enclave Page Cache (EPC)
- Pamięć EPC jest szyfrowana w pamięci głównej (RAM)
- EPC jest zarządzany przez OS / VMM

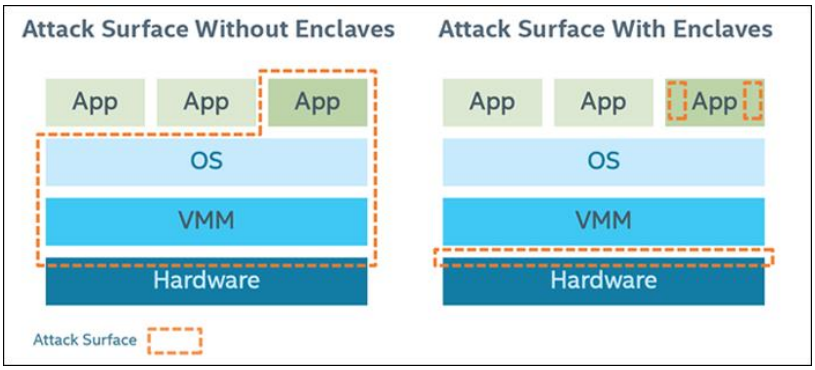
- Zaufany sprzęt składa się tylko z matrycy procesora

Redukcja obszaru ataku dzięki SGX

SGX ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Aplikacja zyskuje możliwość obrony własnych sekretów
  - Mniejszy obszar ataku (enklawa aplikacji + procesor)
  - Złośliwe oprogramowanie, które zagraża OS lub VMM, BIOS-owi, sterownikom nie jest w stanie wykraść sekretów aplikacji

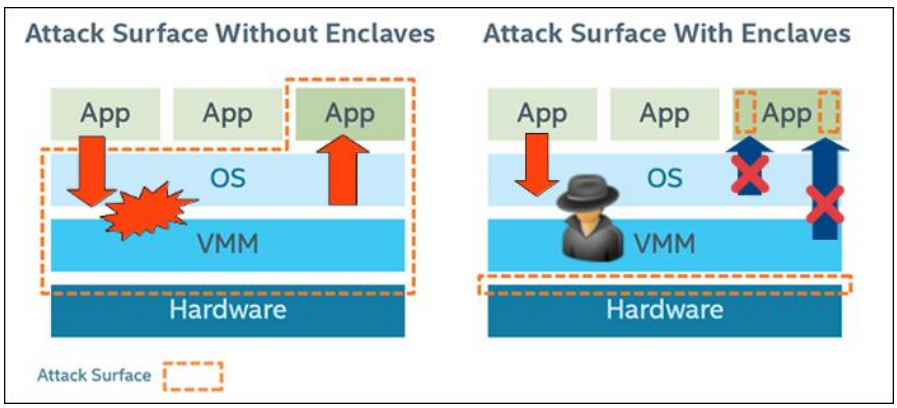


https://software.intel.com/en-us/articles/intel-software-guard-extensions-tutorial-part-1-foundation

Redukcja obszaru ataku dzięki SGX

SGX ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



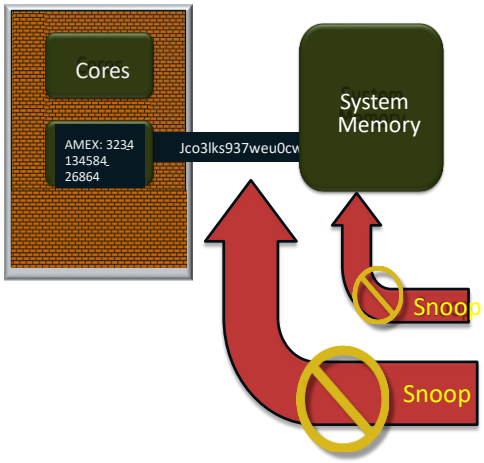
Architektura warstwowa ↔ TCB tylko sprzętowa

https://software.intel.com/en-us/articles/intel-software-guard-extensions-tutorial-part-1-foundation

Ochrona przed szpiegowaniem pamięci

SGX ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



- Obszar bezpieczeństwa to granica pakietu procesora
- Dane i kod są w pakiecie procesora niezaszyfrowane
- Dane i kod poza pakietem procesora są szyfrowane i/lub sprawdzane pod kątem integralności
- Odczytując pamięć zewnętrzną i magistralę szpiedzy widzą tylko zaszyfrowane dane.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

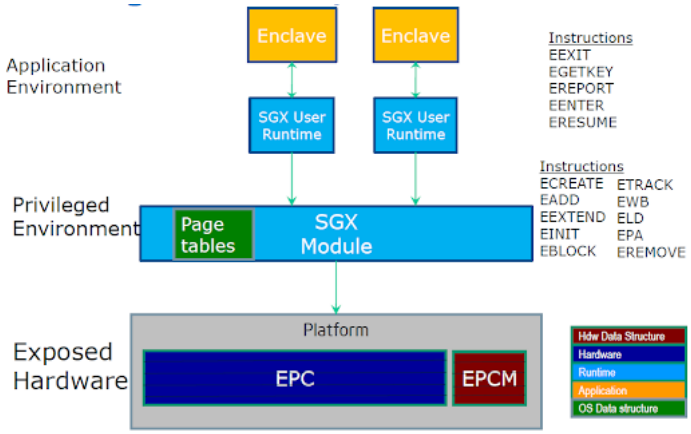
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

33

Ogólny schemat sprzętu/oprogramowania SGX

SGX ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



Pamięć podręczna stron enklawy (EPC) to chroniona pamięć używana do przechowywania stron enklawy i struktur SGX. EPC jest podzielona na fragmenty 4KB zwane stroną EPC. Mapa pamięci podręcznej strony enklawy (EPCM) to chroniona struktura używana przez procesor do śledzenia zawartości EPC.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

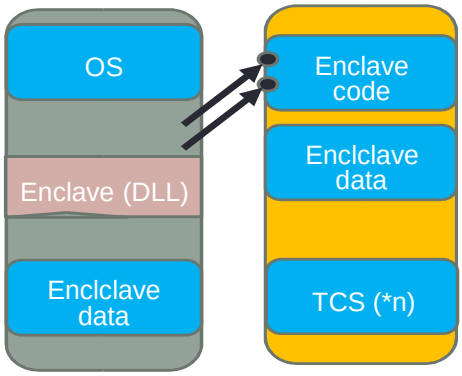
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

34

Środowisko programistyczne SGX

SGX ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



Chronione środowisko wykonawcze osadzone w procesie:

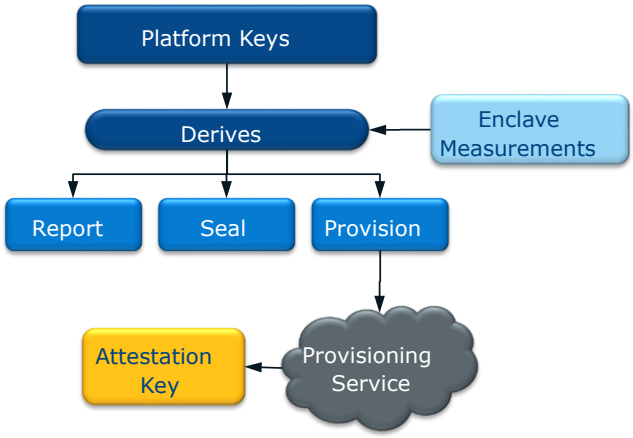
- Z własnym kodem i danymi
- Zapewniające ochronę poufności i integralności
- Z kontrolowanymi punktami wejścia
- Obsługujące wiele wątków
- Z pełnym dostępem do pamięci aplikacji
- Dedykowane punkty wejście do enklawy

TCS= Thread Control Structure

Atestacja i pieczętowanie

SGX ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



- SGX obsługuje operacje **atestacji** enklaw oraz **pieczętowanie** danych w enklawie
- Pojęcia te zostaną wyjaśnione w kolejnym wykładzie o module TPM

Trusted Computing Group (TCG)

TCG ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

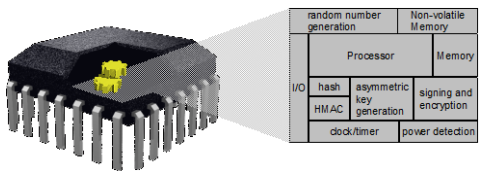
- Grupa założona w 1999 przez firmy Compaq, HP, IBM, Intel i Microsoft
  - Obecnie skupia ponad 200 członków
- Wersje specyfikacji TPM (Trusted Platform Module)
  - TPM 1.0 opublikowana w lutym 2001 r.
  - TPM 1.1b opublikowana w 2003 r.
  - TPM 1.2 rozwijana w latach 2005–2011
  - TPM 2.0 opublikowana w kwietniu 2014 r.
- Aktualnie stosowane specyfikacje TPM
  - Version 1.2 Revision 116, 1 Mar 2011
    - Brak kompatybilności z Version 1.1
  - Version 2.0 Revision 01.38, Version 2.0 Revision 01.38, November 8, 2019 (ISO/IEC 11889:2015, parts 1-4)
- Standardy TPM są opracowywane przez Trusted Computing Group (TCG), www.trustedcomputinggroup.org

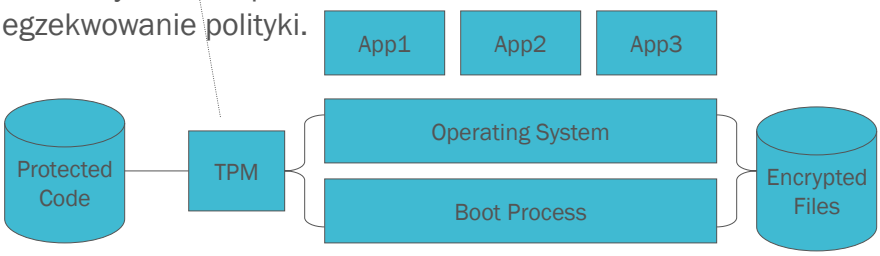
Cooprocesor-based TEE - zaufana architektura obliczeniowa

TPM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- **TPM** (Trusted Platform Module): moduł sprzętowy odporny na manipulacje zamontowany na platformie obliczeniowej.
- **Odpowiedzialny za**: pomiar, przechowywanie, raportowanie i egzekwowanie polityki.

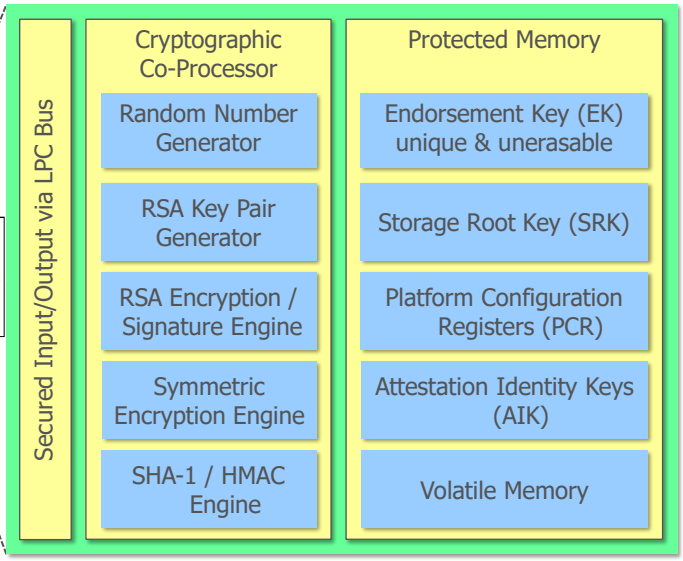




Zaufana architektura obliczeniowa – TPM 1.2

TPM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

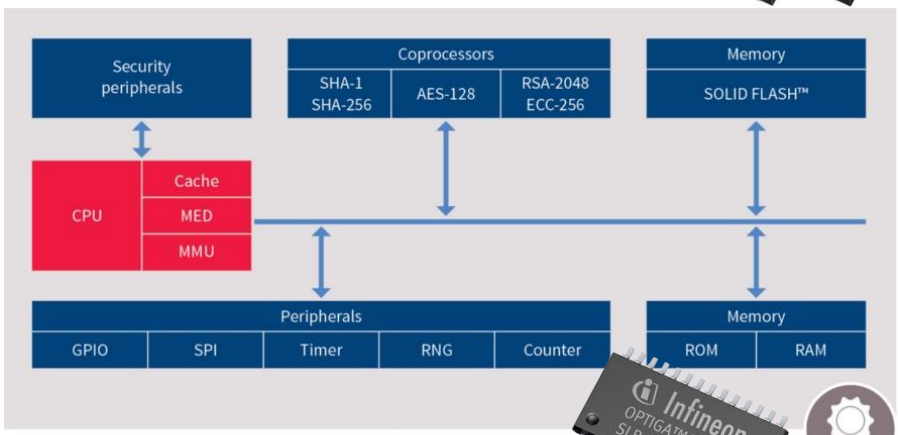
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

39

Zaufana architektura obliczeniowa – TPM 2.0

TPM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

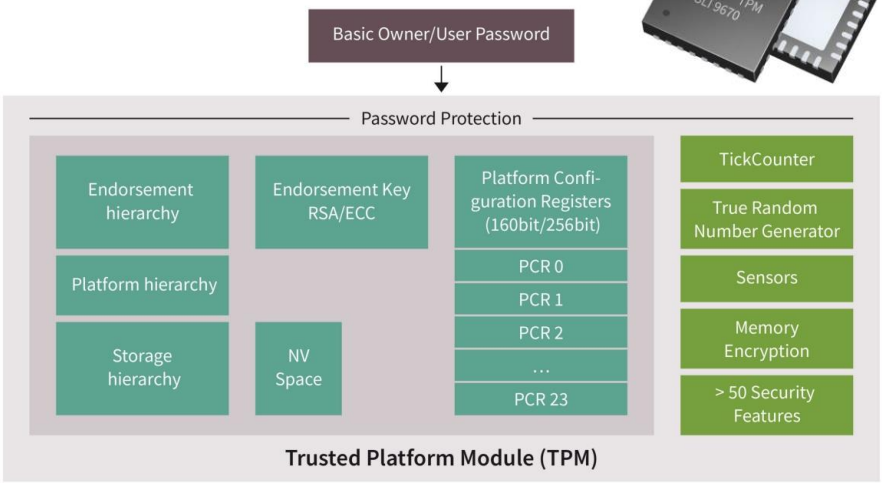
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

40

Zaufana architektura obliczeniowa – TPM 2.0

TPM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

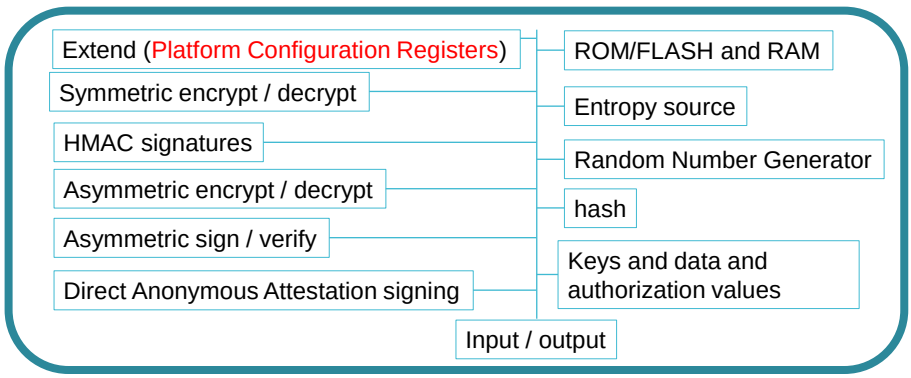
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

41

Co wg TCG zapewnia TPM?

TPM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



Izolacja i odporność na manipulacje

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

42

Zaufana platforma (Trusted Platform, TP) - podsumowanie

TPM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

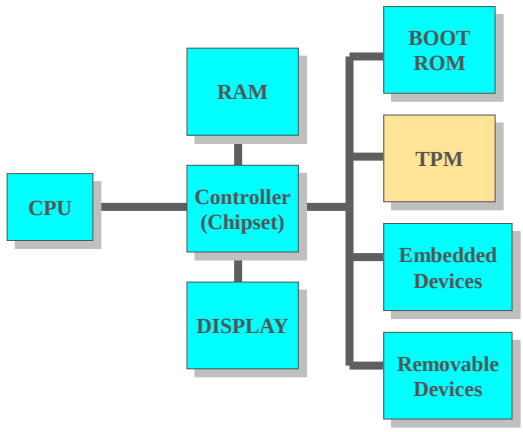
- Zaufane platformy (TP) to platformy komputerowe zawierające zestaw wbudowanych komponentów sprzętowych, które są wykorzystywane jako podstawa do budowania zaufania do oprogramowania.
- Zaufane komponenty to:
  - główne źródło (rdzeń) zaufania do pomiaru (Root of Trust for Measurement RTM), i
  - Zaufany komponent sprzętowy, np. moduł zaufanej platformy (TPM).
- Zaufane komponenty są podłączone na stałe do płyty głównej lub wbudowane w oprogramowanie układowe.

Zaufana platforma (Trusted Platform, TP) – podsumowanie

TPM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

- Zaufana platforma (TP) łączy w sobie mechanizmy zabezpieczenia sprzętu i oprogramowania mające na celu zapewnienia zaufania do urządzenia użytkownika.
- Zaufanie wywodzi się ze sprzętowego zaufanego komponentu, np. TPM.

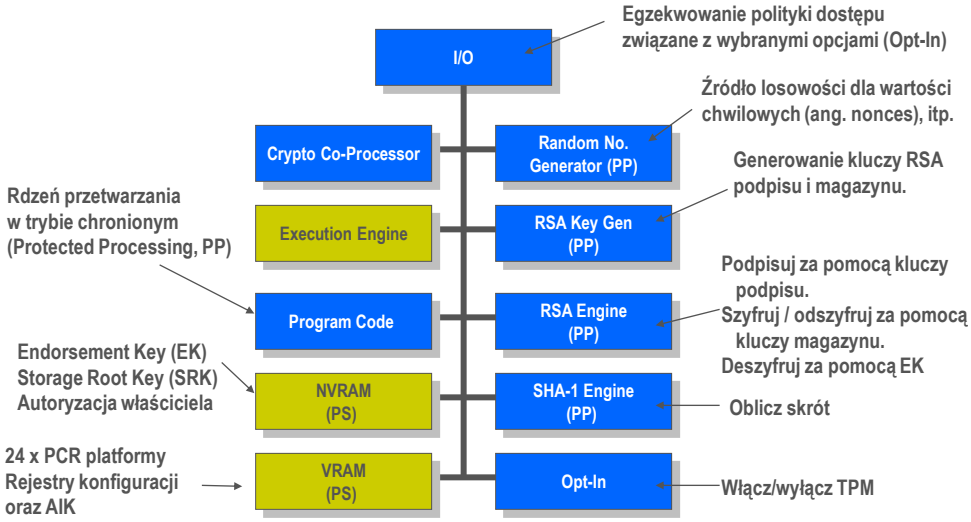


Referencyjna architektura komputera osobistego

Podstawowe własności zaufanej platformy z komponentem TPM 1.2

TPM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



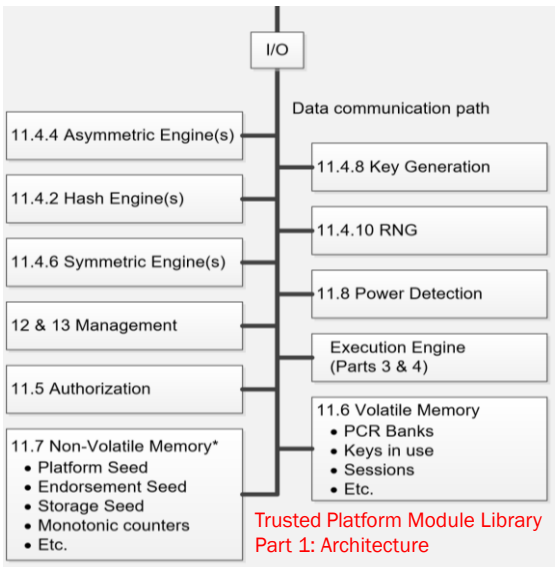
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Podstawowe własności zaufanej platformy z komponentem TPM 2.0

TPM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM ...

- Łańcuch zaufania
- Źródła zaufania
- Metryki i ich pomiary
- Specyfikacje przemysłowe
  - ARM TrustZone
  - Intel Software Guard eXtensions (SGX)
  - Trusted Computing Group (TCG)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Porównanie zaufanych architektur komputerowych opartych na sprzęcie

	Isolation	Attestation	Sealing	Dynamic RoT	Code Confidentiality	Side-Channel Resistance	Memory Protection	Lightweight	Coprocessor	HW-Only TCB	Preemption	Dynamic Layout	Upgradeable TCB	Backwards Compatibility	Open-Source	Academic	Target ISA
AEGIS	●	●	●	●	●	○	●	○	○	●	●	●	○	●	○	●	–
TPM	○	●	●	○	●	–	◓	○	●	●	–	–	○	●	○	○	–
TXT	●	●	●	●	●	●	◓	○	●	●	○	●	○	●	○	○	x86_64
TrustZone	●	○	○	●	○	○	○	○	○	○	●	●	○	●	○	○	ARM
Bastion	●	○	●	●	●	○	●	○	○	○	●	●	●	●	○	●	UltraSPARC
SMART	○	●	○	●	○	–	○	●	○	○	–	–	○	●	○	●	AVR/MSP430
Sancus 1.0	●	●	○	●	○	●	○	●	○	●	○	○	○	●	●	●	MSP430
Soteria	●	●	○	●	●	●	○	●	○	●	○	○	○	●	●	●	MSP430
Sancus 2.0	●	●	○	●	●	●	○	●	○	●	◓	○	○	●	●	●	MSP430
SecureBlue++	●	○	●	●	●	○	●	○	○	●	●	●	○	●	○	○	POWER
SGX	●	●	●	●	●	○	●	○	○	○	●	●	●	●	○	○	x86_64
Iso-X	●	●	○	●	○	○	●	○	○	○	●	●	●	●	○	●	OpenRISC
TrustLite	●	●	○	○	○	●	○	●	○	○	●	●	●	●	○	●	Siskiyou Peak
TyTAN	●	●	●	●	○	●	○	●	○	○	●	●	●	●	○	●	Siskiyou Peak
Sanctum	●	●	●	●	●	●	○	○	○	○	●	●	●	●	◓	●	RISC-V

● = Yes; ◓ = Partial; ○ = No; – = Not Applicable

P. Maene, et al. *Hardware-Based Trusted Computing Architectures for Isolation and Attestation*, IEEE Transactions on Computers, vol. 67, no. 3, pp. 361-374, 1 March 2018,

Jan Tobias Mühlberg "Trusted Execution Environments and how far you can trust them"

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

IIR EXCELLENCE IN RESEARCH

DZIĘKUJĘ ZA UWAGĘ

Wydział Informatyki