Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

IR EXCELLENCE IN RESEARCH

Wydział Informatyki

TRUSTED PLATFORM MODULE (TPM)

dr hab. inż. Jerzy Pejaś, prof. ZUT

Wydział Informatyki

Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie

1

AGENDA

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

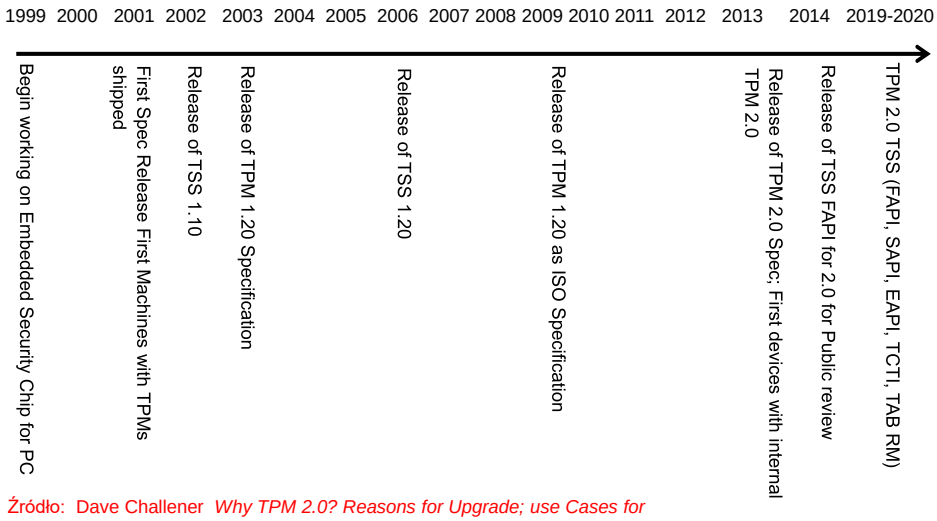
O czym będzie mowa w tym wykładzie?

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły autoryzacji

Specyfikacje techniczne i rozwój TPM

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Źródło: Dave Challener *Why TPM 2.0? Reasons for Upgrade; use Cases for the Latest Release of the TPM Specification*

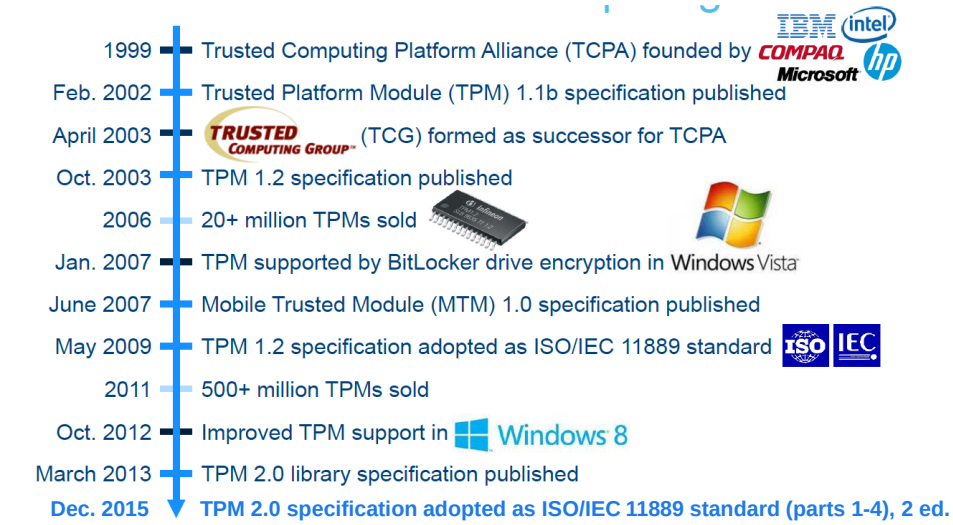
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Kroki milowe rozwoju zaufanych obliczeń

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Źródło: Dries Schellekens, Trusted Platform Module, COSIC, KU Leuven

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Rynek dla TPM

INFORMACJE ...

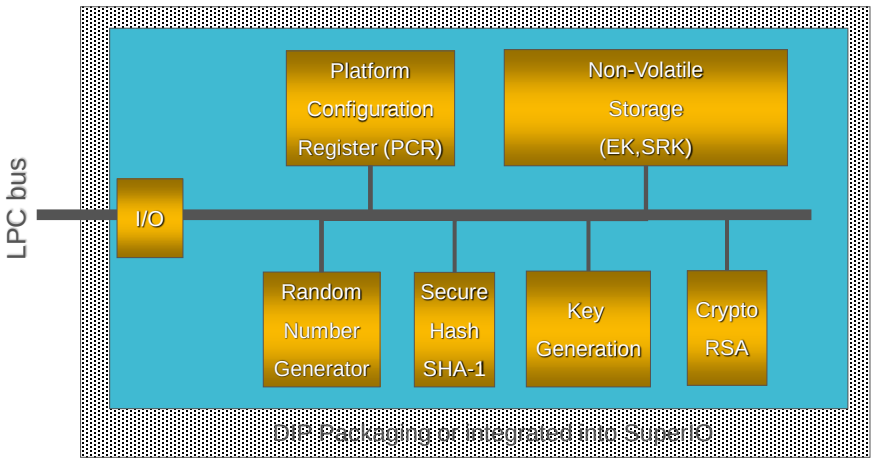
- Informacje o treściach wykładu
- Pojęcia i podstawy zabezpieczeń
- Niektóre aspekty ataków czasu wykonania
- Zaufane obliczenia

- Do tej pory wyprodukowano i wypuszczono na rynek ponad 1 mld urządzeń wyposażonych w układy scalone TPM (v.1.2 i v.2.0)
  - Układy TPM są produkowane przez: Atmel, Broadcom, Infineon, Intel, ITE, Nuvoton, STMicroelectronics, Sinosun, and Toshiba.
  - PC-y z TPM są dostarczane przez firmy Dell, Acer, NEC, Gateway, Lenovo, HP, Intel, Toshiba, Fujitsu.
  - Układy TPM są wspierane przez następujące SO: Windows Vista, Windows 7/8/10, Windows Server 2008/2012/2016/2019, Linux, Mac OS X, Chromium OS.

TCG Trusted Platform Module (TPM)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Produkowane wersje TCG Trusted Platform Module (TPM)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Większość używanych modułów TPM jest produkowanych w wersji TPM 1.2
  - Produkowana była także wersja TPM 1.0, dzisiaj już zapomniana.
- Obecnie produkowana jest nowa wersja TPM 2.0
  - W wielu elementach TPM 2.0 różni się od TPM 1.2
  - TPM 2.0 ma bardziej elastyczne (zwinne) algorytmy
  - TPM 2.0 pozwala elastycznie definiować polityki (reguły) używania obiektów (np. kluczy)
  - Ma trzy oddzielne hierarchie kluczy:
    - Klucze platformy, klucze poręczenia i klucze magazynu
    - Elastyczność sprawia, że TPM 2.0 jest bardziej przydatny, ale może również prowadzić do fragmentacji jego zastosowań.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM – separacja funkcji

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- W TPM 1.2 wszystko jest pod kontrolą „właściciela”
  - Jeśli moduł TPM nie jest włączony, aktywowany i nie należy do użytkownika, który jest jego właścicielem, to niewiele można z nim zrobić
  - Jeśli użytkownik jest właścicielem, to kontroluje zarówno funkcje bezpieczeństwa, jak i prywatność
- W TPM 2.0 istnieją trzy oddzielne domeny
  - Bezpieczeństwo (ang. security) - funkcje chroniące bezpieczeństwo użytkownika
  - Prywatność (ang. privacy) - funkcje chroniące tożsamość platformy/użytkownika
  - Platforma (ang. platform) - funkcje chroniące integralność platformy/usług oprogramowania układowego
- Każda domena ma własne zasoby i mechanizmy kontrolne (m.in. wartości autoryzujące, np. hasła oraz polityki autoryzacji)
  - Bezpieczeństwo – *ownerAuth,* hierarchia magazynu, zezwolenie na tworzenie hierarchii (*shEnable*=ON/OFF).
  - Prywatność – *endorsmentAuth,* hierarchia poręczenia, *ehEnable*=ON/OFF.
  - Platforma - *platformAuth*, hierarchia platformy, *phEnable*=ON/OFF.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM - hierarchie

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

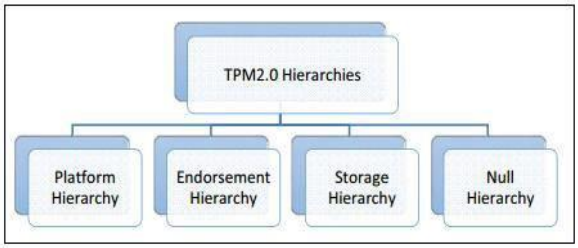
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM 1.2

Pojedyncza hierarchia:

- hierarchia magazynu
  - dla użytkownika platformy



TPM 2.0

Cztery hierarchie:

- hierarchia platformy (TPM_RH_PLATFORM) - dla oprogramowania układowego
- hierarchia magazynu (TPM_RH_OWNER) - dla użytkownika platformy
- hierarchia poręczenia (TPM_RH_ENDORSEMENT) - dla administratora platformy
- hierarchia pusta (ang. null hierarchy)) (*TPM_RH_NULL*) – dla każdego

TPM 2.0 - hierarchie

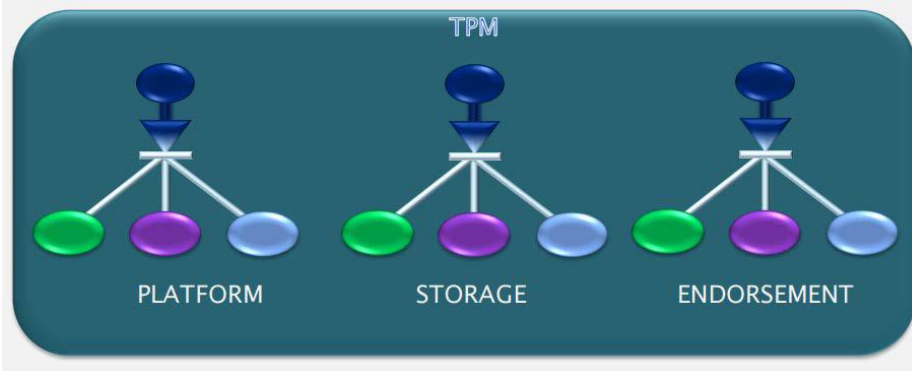
INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

HR EXCELLENCE IN RESEARCH

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki



TPM 2.0 – hierarchia platformy

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Dla oprogramowania układowego platformy BIOS/UEFI
- Po uruchomieniu platformy hierarchia platformy jest włączona, a *platformAuth* jest ustawiana na nową wartość
  - Umożliwia korzystanie z modułu TPM w celu zapewnienia integralności oprogramowania sprzętowego
  - To nie jest hierarchia, którą powinien kontrolować użytkownik, więc tak nie jest (kontroluje ją producent modułu TPM)
- *platformAuth* może służyć do:
  - Alokowania zasobów w pamięci nieulotnej
  - Inicjalizowania modułu TPM
  - Kontrolowania uaktywniania innych hierarchii
- Zanim oprogramowanie układowe platformy przekaże sterowanie systemowi operacyjnemu, można wyłączyć *phEnable* lub randomizować *platformaAuth*
  - p*latformAuth* zostanie umieszczony w bezpiecznej lokalizacji, tak aby tylko oprogramowanie układowe platformy mogło uzyskać do niego dostęp

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM 1.2 i 2.0 – hierarchia magazynu

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Dla użytkownika (właścicielea) platformy
- Hierarchia magazynu TPM 2.0 jest odpowiednikiem hierarchii magazynu w TPM 1.2.
- Posiada politykę właściciela i wartość autoryzacji, które pozostają niezmienione po ponownym uruchomieniu TPM.
- Hierarchia może zostać wyłączona przez właściciela bez wpływu na hierarchię platformy. Pozwala to oprogramowaniu platformy na używanie modułu TPM, nawet jeśli właściciel wyłączy swoją hierarchię.
  - W TPM 1.2 wyłączenie pojedynczej hierarchii magazynu powodowało wyłączenie modułu TPM.
- Podobnie, hierarchię można wyczyścić (zmieniając podstawowe ziarno i usuwając trwałe obiekty) niezależnie od innych hierarchii.
- Hierarchia magazynu jest przeznaczona do wykonywania operacji, które nie wpływają na utratę prywatności TPM, podczas gdy hierarchia poręczenia, z oddzielnymi mechanizmami kontroli, dotyczy prywatności.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM 2.0 – hierarchia poręczenia

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Jest to hierarchia chroniąca prywatność platformy i znajduje się pod kontrolą administratora prywatności, który może być użytkownikiem końcowym.
- Moduł TPM i administrator zaświadczają, że klucze podstawowe w tej hierarchii są przypisane do autentycznego modułu TPM dołączonego do autentycznej platformy.
- Klucze poręczenia (ang. endorsment keys, EKs).
  - Tyle ile jest potrzebnych
  - Tworzone z sekretnego ziarna (ang. seed)
  - Mogą służyć do składania podpisów
  - Mogą być używane z różnymi algorytmami
  - Należą do własnej hierarchii kluczy
  - Przykłady:
    - można utworzyć klucz podpisujący EK, podpisać CSR (ang. Certificate Signing Request) i uzyskać certyfikat urządzenia bezpośrednio od urzędu certyfikacji;
    - jeśli EK ma poświadczenie (certyfikat), to za pomocą EK nie powinno być możliwości złożenia podpisu (chroni to prywatność TPM).

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM 2.0 – hierarchia pusta

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Jest jak pozostałe hierarchie, ale nie można jej wyłączyć; w ramach tej hierarchii modułu TPM używa się w trybie koproocesora kryptograficznego.
  - W ramach tej hierarchii wartości autoryzacji i polityk są zawsze równe NULL.
- Ziarno hierarchii zerowej nie jest trwałe i po każdym ponownym uruchomieniu modułu TPM generowane jest nowe ziarno o innej wartości.
  - Tak więc z tego ziarna można tworzyć nowe obiekty podstawowe.
- Klucze, które mają część publiczną i prywatną, powinny być zazwyczaj ładowane w hierarchii pustej z dwóch powodów;
  - jest zawsze włączona, i
  - brak autoryzacji (hasło o zerowej długości).

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM 2.0 – typy autoryzacji

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Moduł TPM obsługuje trzy metody autoryzacji bazujące na wartościach autoryzacji:
  - **hasło**;
  - kod uwierzytelniający skrót wiadomości (**HMAC**);
  - **polityki autoryzacji**.
- Hasła i autoryzacja HMAC autoryzują polecenia i funkcje TPM w oparciu o znajomość sekretu przechowywanego w urządzeniu TPM.
- Metoda autoryzacji oparta na politykach, znana również pod nazwą zaawansowana autoryzacja (ang. *enhanced authorization*, EA), autoryzuje polecenia i funkcje TPM na podstawie odpowiednio sformułowanych warunków (nazywanych asercjami polityk).
  - Asercje te można łączyć za pomocą operatorów logicznych AND i OR (np. “określony stan rejestru konfiguracji platformy (PCR)” AND “poprawny sekret”).
  - Asercje polityk są poleceniami wysyłanymi do modułu TPM w celu autoryzacji działania na obiekcie.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM 2.0 – Enhanced Authorization (EA)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Twórca obiektu, korzystając z rozszerzonego mechanizmu autoryzacji EA, może wymagać wykonania określonych testów lub działań (**autoryzacji**) zanim określone polecenie TPM uzyska prawo odwołania się do tego obiektu.
- Specyficzne wymagania, zdefiniowane w formie *równania polityki*, zawarte są w wartości o nazwie *authPolicy* umieszczonej w strukturze danych obiektu.
  - Gdy twórca obiektu ustawi wartość *authPolicy*, nie można go zmodyfikować.
- Aby użyć obiektu, użytkownik powinien najpierw uruchomić *sesję polityki* znajdującą się w chronionej pamięci modułu TPM, a następnie wywołać sekwencję poleceń związanych z asercjami polityk w celu zakończenia testów wymaganych przez politykę. Polecenia te sprawdzają asercje i modyfikują *policyDigest* sesji oraz inne wartości kontekstu.

$$polID_{new} := \text{Hash}(polID_{old} || polLabel_{new} || Param_{new})$$

$polLabel_{new}$ – ID nowej asercji polityki (np. 'PCR'), $Param_{new}$ – parametry związane z asercją (np. pożądana wartość rejestru PCR)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM 2.0 – Enhanced Authorization (EA)

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

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- *Password (in the clear)*: This was missing in TPM 1.2. In some environments, such as when BIOS has control of a TPM before the OS has launched, the added security obtained by using a hash message authentication code (HMAC) doesn't warrant the extra software cost and complexity of using an HMAC authorization to use the TPM's services.
- *HMAC key (as in 1.2)*: In some cases, particularly when the OS that is being used as an interface to talk with the TPM isn't trusted but the software talking to the TPM *is* trusted, the added cost and complexity of using an HMAC for authorization is *warranted*. An example is when a TPM is used on a remote system.
- *Signature (for example, via a smart card)*: When an IT employee needs to perform maintenance on a TPM, a smart card is a good way to prevent abuse of an IT organization's privileges. The smart card can be retrieved when an employee leaves a position, and it can't be exposed as easily as a password.
- *Signature with additional data*: The extra data could be, for example, a fingerprint identified via a particular fingerprint reader. This is a particularly useful new feature in EA. For example, a biometric reader can report that a particular person has matched their biometric, or a GPS can report that a machine is in a particular region. This eliminates the TPM having to match fingerprints or understand what GPS coordinates mean.
- *PCR values as a proxy for the state of the system, at least as it booted*: One use of this is to prevent the release of a full-disk encryption key if the system-management module software has been compromised.
- *Locality as a proxy for where a particular command came from*: So far this has only been used to indicate whether a command originated from the CPU in response to a special request, as implemented by Intel TXT and AMD in AMD-v. Flicker, a free software application from Carnegie Mellon University, used this approach to provide a small, secure OS that can be triggered when secure operations need to be performed.
- *Time*: Policies can limit the use of a key to certain times. This is like a bank's time lock, which allows the vault to be opened only during business hours.
- *Internal counter values*: An object can be used only when an *internal counter is* between certain values. This approach is useful to set up a key that can only be used a certain number of times.
- *Value in an NV index*: Use of a key is restricted to when certain bits are set to 1 or 0. This is useful for revoking access to a key.
- *NV index*: Authorization is based on whether the NV index has been written.
- *Physical presence*: This approach requires proof that the user is physically in possession of the platform.

Wszystkie te formy autoryzacji można również łączyć ze sobą otrzymując bardziej złożone polityki dostępu.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM 2.0 – Enhanced Authorization (EA)

TPM Library Part 3: Commands

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Polecenia dotyczące polityk autoryzacji mają nazwy w postaci **TPM2_PolicyXXX()**, gdzie „XXX" oznacza etykietę typu asercji polityki

Label	Actions	Description of assertion	classification
NV	validate selected NV (Non-Volatile) update polD (policyDigest)	NV Index has the desired relationship with the input value	Immediate
PCR	validate selected pcr update polD, pcrUpdateCounter	Selected pcr has the desired value	Combined
CounterTimer	validate internal clock update polD	Internal clock has the desired relationship with the input value	Immediate
CpHash	update polD, cpHash	Auth for commands with a specified cpHash	Deferred
NameHash	update polD, nameHash	Auth for commands with a specified nameHash	Deferred
CommandCode	update polD, commandCode	Auth for a specified command	Deferred
DuplicationSelect	update polD, cpHash, commandCode	Auth for TPM2_Duplicate with a specified cpHash	Deferred
AuthValue	update polD, isAuthValueNeeded	an HMAC keyed on the authValue required	Deferred
Password	update polD, isPasswordNeeded	a password required	Deferred
Locality	update polD, locality	Auth for commands executed at specified locality	Deferred
PhysicalPresence	update polD, isPPRequired	physical presence required	Deferred
NvWritten	update polD, checkNvWritten, NvWrittenState	NV Index has the desired attribute for written	Deferred
Signed	validate signature of param update polD, timeout	Auth bound with session (used once), specified polRef, expiration for auth	Combined
Secret	validate HMAC of param update polD, timeout	Auth bound with session (used once), specified polRef, expiration for auth	Combined
Ticket	validate tickets for specific authorization update polD, timeout	specified cpHash, expiration for auth	Combined
Authorize	validate and update polD	polD has been signed by a specified key	Authorize
OR	validate and update polD	polD is in the list of digest	OR

J. Shao, Y. Qin, D. Feng, W. Wang *Formal Analysis of Enhanced Authorization in the TPM 2.0*, ASIA CCS'15, April 14–17, 2015, Singapore

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Logika polityki autoryzacji

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Politykę można zapisać jako równanie, w którym każdy element składowy (asercja) jest łączony za pomocą operatorów logicznych AND (&) i OR (I).
- Przykład: (A & B & C) I (D & E & F)
  - Z grubsza rzecz biorąc, lewa strona równania obliczana jest następująco:

    $skrót_{lewy}$: = Hash (Hash (Hash (0 ‖ A) ‖ B) ‖ C)
  - zaś prawa strona tak:

    $skrót_{prawy}$: = Hash (Hash (Hash (0 ‖ D) ‖ E) ‖ F)

Uwaga: obliczenia Hash (Hash (Hash (O ‖ C) ‖ B) | | A) dają zupełnie inną wartość niż $skrót_{lewy}$.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

19

TPM - algorytmy kryptograficzne

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

TPM 1.2

- RSA encryption
- RSA signature
- RSA-DAA
- SHA-1
- HMAC
- One-time-pad with XOR
- AES (optional)

TPM 2.0

- RSA encryption and signature
- ECC encryption and signature
- ECC-DAA
- ECDH
- SHA-1, SHA-256
- HMAC
- AES-128/256 (ECB/CBC/CFB/OFB/CTR/ CMAC)
- Producent może dodać dowolne algorytmy z identyfikatorami TCG

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

20

Dlaczego odchodzi się od TPM 1.2 do TPM 2.0?

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Bezpieczeństwo
  - TPM 1.2 został zbudowany wokół SHA-1
    - Algorytm został osadzony we wszystkich strukturach
    - Nie było wystarczająco dużo miejsca, aby go po prostu zmienić na SHA-256
- Złożoność
  - TPM 1.2 urósł „organicznie” po wersji 1.1b
  - To było niepotrzebnie skomplikowane
- Łatwość użycia
  - TPM 1.2 jest trudny w użyciu
  - Złożoność autoryzacji
- Potrzeba nowych funkcjonalności
  - Elastyczność algorytmu
  - Ujednolicona autoryzacja
  - Szybkie ładowanie klucza

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

21

Dlaczego warto korzystać z TPM 2.0?

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Eliminuje ograniczoność entropii prowadzącej do słabych kluczy
- Obniża ryzyko związane z łańcuchem dostaw/podrabiany sprzęt
- Pozwala na trzymanie złych facetów z dala od wewnętrznej sieci
- Pozwla na trzymanie złośliwego oprogramowania infekującego sprzęt poza siecią wewnętrzną
- Zapobiega masowemu ujawnianiu baz haseł
- Pozwala na uwierzytelnianie wieloskładnikowe
- Zapewnia bezpieczeństwo poczty e-mail
- Zawiera silniki szyfrujące z certyfikatem FIPS/Common Criteria
- Pozwala na zabezpieczanie kluczy głównych certyfikatów użytkownika
- Łączy w sobie kontrolę fizyczną i logiczną

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

22

Dlaczego warto korzystać z TPM 2.0? Uwierzytelnianie wieloskładnikowe

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania





Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

23

Dlaczego warto korzystać z TPM 2.0? Uwierzytelnianie wieloskładnikowe

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- ❑ Sposoby uwierzytelnienia
  - Hasła są słabe (zwłaszcza same w sobie)
    - Słabe hasła można łatwo złamać
  - Biometria jest słaba (zwłaszcza sama w sobie)
    - Spoofing biometryczny to wyścig zbrojeń
  - „To co posiadasz” może zostać utracone
    - Uwierzytelnianie dobre w zapobieganiu atakom zdalnym (szczególnie na bardzo duże odległości), ale nie radzi sobie z *Grand Chess Attack*
  - Godzina dnia /lokalizacja GPS/unieważnianie/ n-krotna autoryzacja
    - Zwykle dobre w szczególnych przypadkach użycia, ze wszystkimi związanymi z tym potencjalnymi problemami
- ❑ Rozwiązanie
  - Użyj więcej niż jednego składnika uwierzytelniania!

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

24

Zaawansowane uwierzytelnianie za pomocą TPM 2.0

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

- Wszystkie usługi w module TPM można skonfigurować za pomocą projektanta uwierzytelniania
  - od jedno- do n-składnikowego uwierzytelniania (prostego lub złożonego)
  - dowolny rodzaj uwierzytelnienia, o jakim tylko można pomyśleć
- Usługi mogą mieć dowolną ziarnistość!
  - mogą odnosić się nie tylko do pojedynczego obiektu
  - mogą operować na każdym obiekcie
- Przykłady
  - Klucze, które można powielać TYLKO na określonych serwerach
  - Klucze, które mogą być duplikowane TYLKO przez określonych administratorów
  - Klucze, których można używać tylko po uprzedniej oddzielnej autoryzacji przez dwa różne organy
  - Klucze powiązane z określonymi urządzeniami zewnętrznymi (biometria, zegary, GPS)

Uwierzytelnianie wieloskładnikowe (c.d.)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

- Nowe mechanizmy uwierzytelnienia w TPM pozwalają na praktycznie dowolne limitowanie dostępu do usług TPM
- Przykłady
  - Jeden użytkownik może być zobowiązany do spełnienia kilku kryteriów uwierzytelnienia
    - Biometria
    - Smartcards
    - Hasła/HMAC
    - Stan maszyny
    - Położenie wg GPS
    - Itd..
  - Wielu użytkowników może uwierzytelnić się osobno za pomocą tego samego klucza
  - Zadania administracyjne dotyczące zarządzania kluczami (takie jak duplikacja) można autoryzować niezależnie od zwykłych zadań użytkownika.

Dlaczego warto korzystać z TPM 2.0? Zabezpieczanie głównych certyfikatów użytkownika

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Bezpieczny magazyn – pamięć nieulotna (Non-Volatile, NV) miejsca do przechowywania sekretów (np. haseł) lub informacji statycznych

- NV może służyć do przechowywania dowolnych informacji
  - W fazie uruchamiania systemu NV może być dostępna tylko dla z góry zdefiniowanego systemu operacyjnego
- NV może służyć do przechowywania certyfikatów/kluczy, które reprezentują maszynę lub certyfikaty głównych urzędów certyfikacji (CA)
- NV może przechowywać „złote pomiary" (ang. golden measurements) systemu, np. dostarczone z systemem
- NV może służyć do przechowywania identyfikatorów udostępniania
  - Oprogramowanie, które powinno zostać zainstalowane w systemie podczas udostępniania
  - Wymagania bezpieczeństwa systemu
- Uprawnienia do odczytu/zapisu są „usługami", które mogą podlegać takim samym ograniczeniom, jak inne usługi TPM.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

27

Trzy podstawowe zadania zaufanej platformy TCG

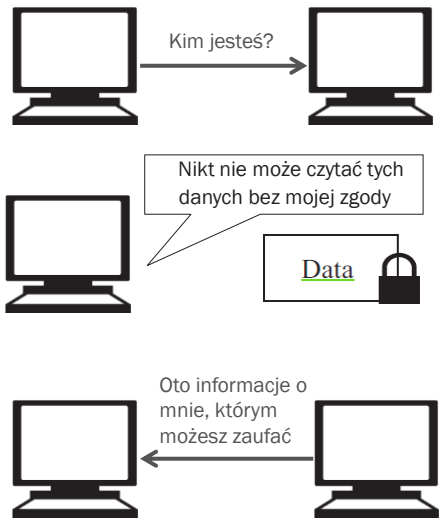
INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Uwierzytelnianie maszyn (ang. machine authentication) – polega na identyfikacji tożsamości maszyny w oparciu o przypisany jej klucz kryptograficzny.

Ochrona danych (ang. data protection) - polega na wykorzystaniu TPM jako sprzętowego głównego punktu zaufania (RoT) do szyfrowania dysku i ochrony dużych plików oraz wykorzystania nieulotnej pamięci wewnętrznej TPM danych wrażliwych o niedużych rozmiarach (np. kluczy)

Atestacja (ang. attestation) - proces weryfikacji dokładności informacji i metryk aktualnego stanu TPM



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

28

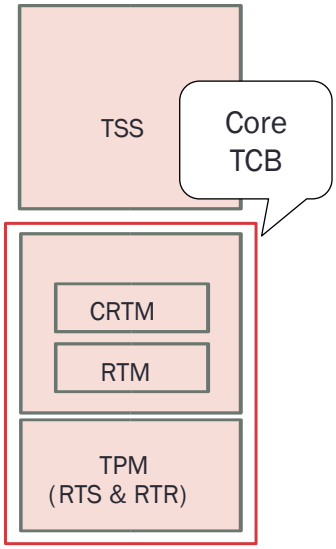
Główne elementy systemu z modułem TPM

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Trusted Compute Base (TCB)
  - Root of Trust for Measurement (RTM)
  - Core Root of Trust for Measurement (CRTM)
  - Statyczny i dynamiczny RTM (S-RTM, D-RTM)
- Root of Trust for Storage (RTS)
- Root of Trust for Reporting (RTR)
- TCG Software Stack (TSS)

TPM nie jest zaufaną bazą obliczeniową systemu. TPM jest raczej komponentem, który pozwala niezależnemu podmiotowi określić, czy TCB został skompromitowany. W niektórych zastosowaniach TPM może pomóc w zapobieganiu uruchomieniu systemu, jeśli TCB nie może być prawidłowo zainicjowany.



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

29

CRTM, S-RTM i D-RTM

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- CRTM jest *a priori* zaufanym kodem, który jest częścią poświadczeń platformy. W stacjach roboczych *CRTM = blok rozruchowy BIOS*.
- W modelu S-RTM, CRTM musi być pierwszym fragmentem kodu wykonywanym po włączeniu zasilania lub zresetowaniu serwera lub kompletnego fizycznego środowiska sprzętowego.
  - Uwaga: podczas uruchamiania, CRTM sprawdza fizyczną obecność modułu TPM
  - Uwaga! TPM nie jest głównym źródłem zaufania (RoT). Zaufanie zaczyna się od CRTM.
- W modelu D-RTM sprzęt został zaprojektowany tak, aby podczas uruchamiania rozpoczęte zostało wykonywanie zaufanego wątku:
  - **Intel** nazywa swoją technologię Trusted eXecution
  - **AMD**: instrukcje DRTM, SKINIT

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

30

CRTM, S-RTM i D-RTM (c.d.)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Punktem startowym pomiaru jest rdzeń głównego punktu zaufania (Core Root of Trust for Measurement, CRTM). Proces ten dokonuje wstępnych pomiarów platformy, które są rozszerzane w PCR platformy TPM.
  - Aby pomiary były sensowne, wykonujący się kod musi kontrolować środowisko, w którym działa, tak aby wartości zarejestrowane w module TPM były reprezentatywne dla początkowego stanu zaufania platformy.
- Po włączeniu urządzenia operacja resetowania tworzy środowisko, w którym platforma znajduje się w znanym stanie początkowym, a CPU wykonuje kod z dobrze zdefiniowanej lokalizacji początkowej. Ponieważ w tym czasie kod ten ma wyłączną kontrolę nad platformą, może dokonywać pomiarów platformy w oparciu o oprogramowanie układowe. Na podstawie tych wstępnych pomiarów można zbudować łańcuch zaufania.
  - Ponieważ łańcuch ten jest tworzony raz po zresetowaniu platformy, nie jest możliwa zmiana początkowego stanu zaufania, dlatego nazywa się go statycznym RTM (S-RTM).
- W przypadku alternatywnej metody inicjalizacji platformy CPU może działać jako CRTM i stosować zabezpieczenia do części pamięci, które mierzy. Ten proces umożliwia rozpoczęcie nowego łańcucha zaufania bez ponownego uruchamiania platformy. Ponieważ RTM można przywrócić dynamicznie, metoda ta nazywa się dynamicznym RTM (D-RTM).
  - Zarówno S-RTM, jak i D-RTM mogą przejąć system w nieznanym stanie i przywrócić go do znanego stanu. D-RTM ma tę zaletę, że nie wymaga ponownego uruchamiania systemu.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Bezpieczny a zaufany rozruch systemu

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Zaufany rozruch (ang. trusted boot) różni się od bezpiecznego rozruchu (ang. secure boot).
- W bezpiecznym rozruchu uruchomiony komponent musi uwierzytelnić następny komponent.
  - Bezpieczny rozruch zatrzyma platformę, jeśli uwierzytelnienie zakończy się niepowodzeniem.
- W zaufanym rozruchu uruchomiony komponent musi obliczyć metrykę następnego komponentu przed jego załadowaniem i uruchomieniem oraz zapisać ją w rejestrze PCR modułu TPM.
  - Rozruch w trybie zaufanym nie kończy się niepowodzeniem, ponieważ podczas uruchomienia nie jest wykonywana żadna weryfikacja metryk.
  - Gdy system zakończy rozruch inne oprogramowanie przeprowadza atestację zmierzonych komponentów w celu sprawdzenia , czy ich obecny stan jest taki sam jak poprzedni. Jeśli tak, to rozruch zaufany można uznać za bezpieczny.

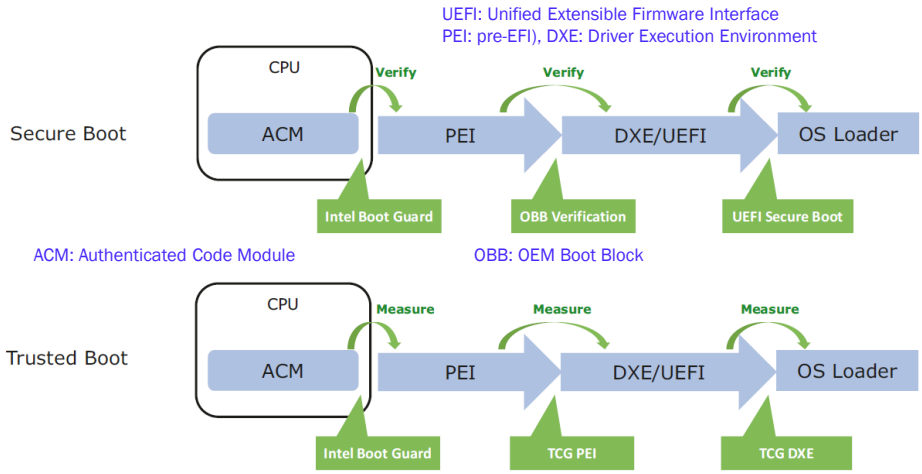
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Bezpieczny a zaufany rozruch systemu

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

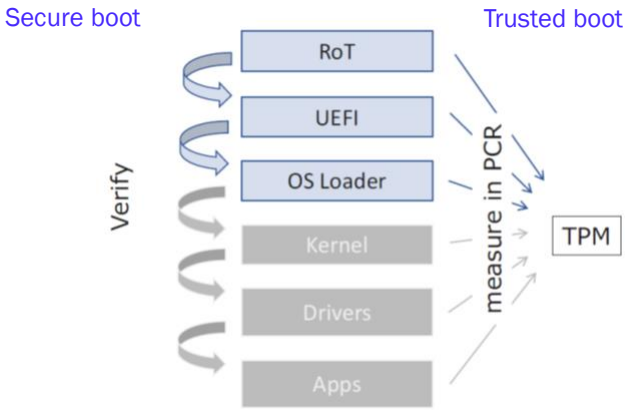
Wydział Informatyki

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

Bezpieczny a zaufany rozruch systemu

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

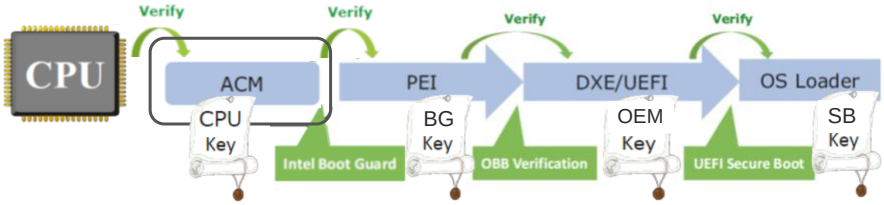
Wydział Informatyki

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

Bezpieczny rozruch systemu

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



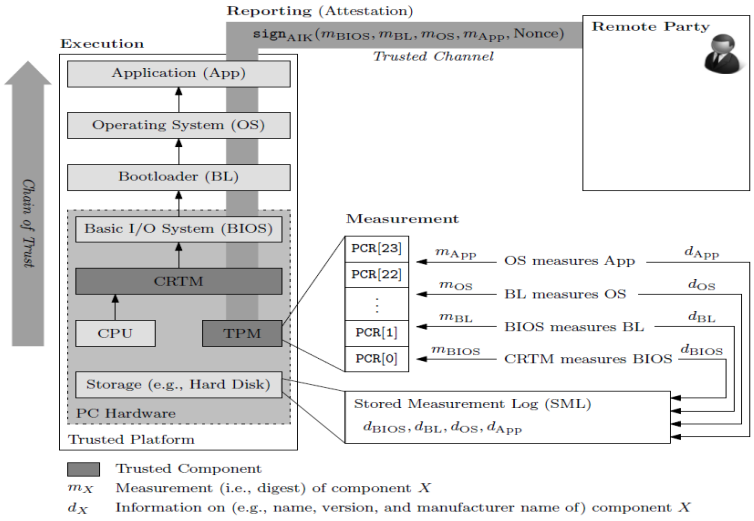
Przebieg weryfikacji bezpiecznego rozruchu

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

Idea zaufanego uruchamiania systemu

INFORMACJE ...

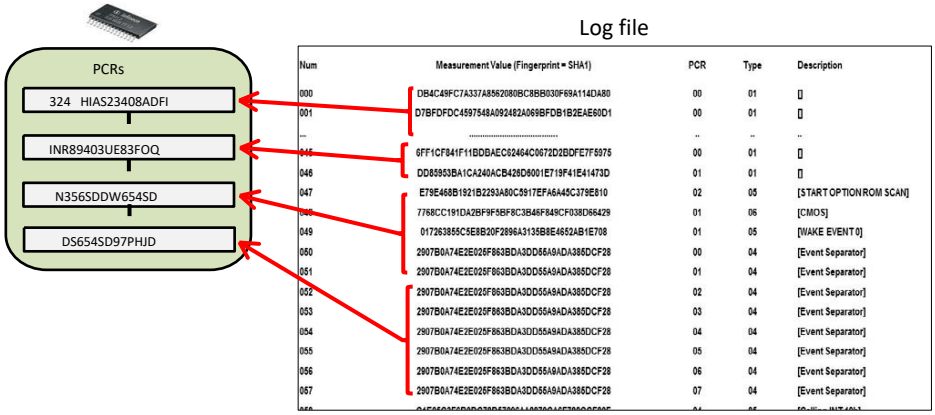
- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Ochrona integralności SML (Stored Measurement Log)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



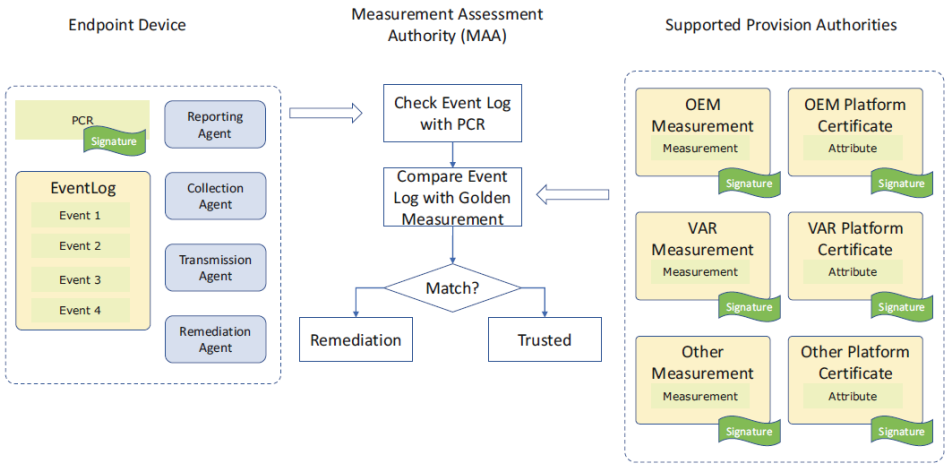
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Atestacja w oparciu o dziennik zdarzeń, PCR i „złote metryki”

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



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

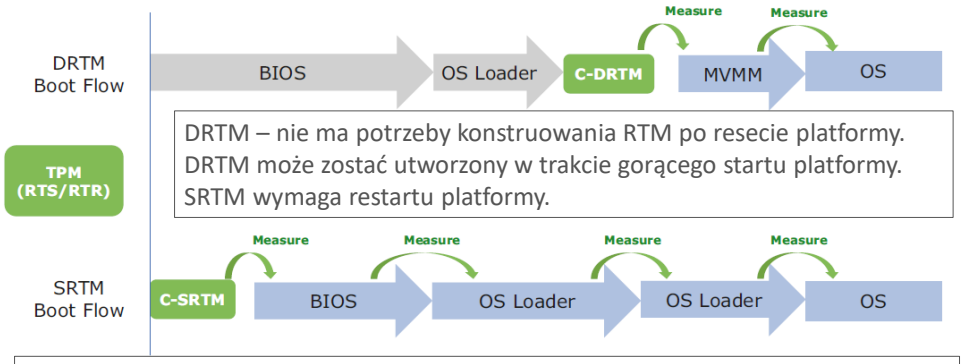
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Modele zaufania S-RTM i D-RTM – uruchamianie systemu

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



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

Cechy TPM 1.2

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Główne cele TPM
  - „Kotwica” zabezpieczeń wewnątrz systemu
  - Pieczętowanie/wiązanie określonej konfiguracji Platformy
  - Atestacja stanu platformy
- Każdy TPM ma unikalny klucz zwany kluczem poręczenia (ang. **Endorsement Key**, EK)
- TPM 1.2 ma 8 stanów:

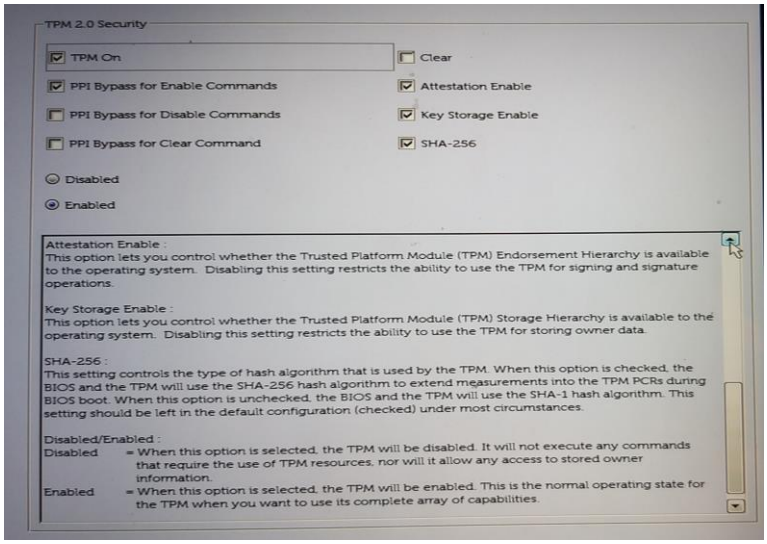
Modes of Operation:

S1 – Enabled – Active – Owned
S2 – Disabled – Active – Owned
S3 – Enabled – Inactive – Owned
S4 – Disabled – Inactive – Owned
S5 – Enabled – Active – Unowned
S6 – Disabled – Active – Unowned
S7 – Enabled – Inactive – Unowned
S8 – Disabled – Inactive - Unowned

Aktywowanie TPM 2.0 (laptop firmy Dell)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Kombinacje ustawień kontrolowania hierarchii w TPM 2.0
(za pomocą polecenia tpm2_hierarchycontrol)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Hierarchy enable	auth Value	auth Policy	Description
SET	Known	Set	The hierarchy is enabled, and objects in it may be loaded. Either authValue or authPolicy may manage resources related to the hierarchy.
SET	Unknown	Set	The authValue may be made unknown by setting it to a random value and then discarding the value. This prevents the authValue from being used. This combination is useful for keeping the hierarchy enabled but using a policy-based delegation scheme for managing hierarchy related resources.
SET	Known	Empty	When the authPolicy is empty, it cannot match any *policyDigest* value so the use of authPolicy is disabled. This combination is most analogous to the control scheme of TPM 1.2, where an authValue (ownerAuth) is used to manage the resources of the single hierarchy supported by a 1.2 TPM.
CLEAR	N/A	N/A	When an enable is FALSE, the corresponding authValue and authPolicy may not be used to authorize any TPM action.

phEnable, platformAuth, platformPolicy, phEnableNV for platform firmware;
shEnable, ownerAuth, ownerPolicy for the Owner
ehEnable, endorsementAuth, endorsementPolicy for the Privacy Administrator.

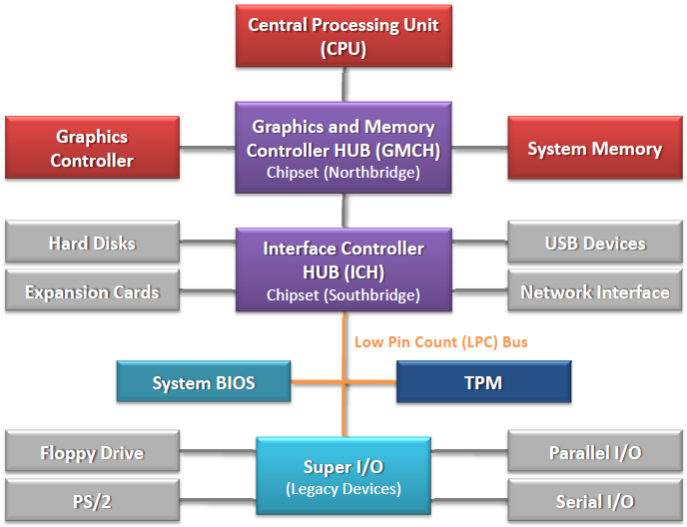
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Integracja TPM ze sprzętem typowego PC

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

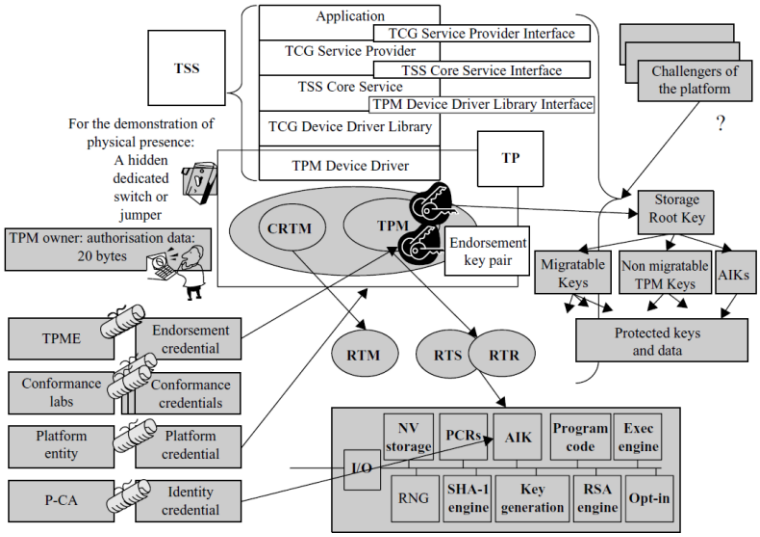


Source: Prof. Dr.-Ing. Ahmad-Reza Sadeghi, Ruhr University Bochum

Zaufana platforma (TPM 1.2)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

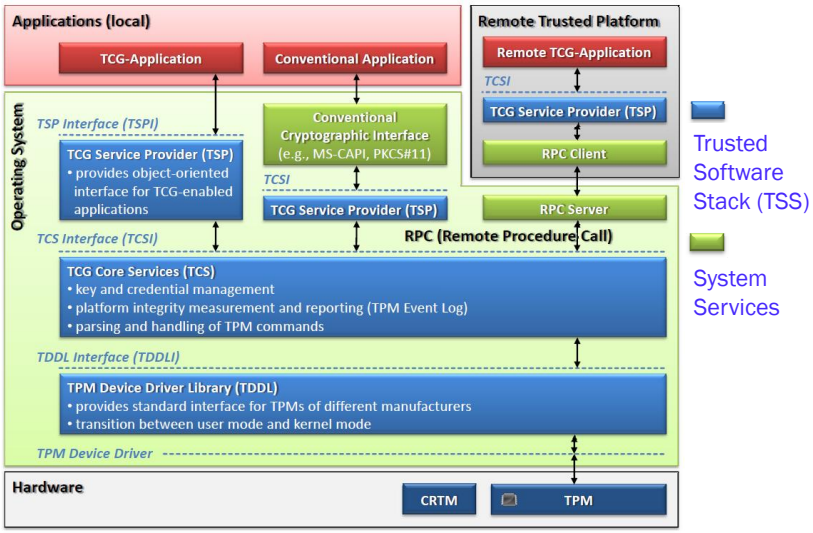


Chris Mitchell *Trusted Computing*

Integracja oprogramowania TPM 1.2

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

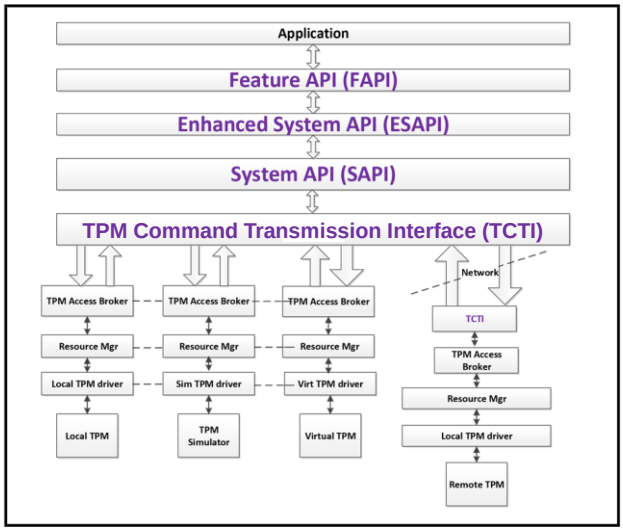


Source: Prof. Dr.-Ing. Ahmad-Reza Sadeghi, Ruhr University Bochum

Integracja oprogramowania TPM 2.0

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



TCG TSS 2.0 Overview and Common Structures Specification

Typy kluczy TPM 1.2

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- W module TPM 1.2 dostępnych jest 9 różnych typów kluczy
  - 3 specjalne typy kluczy TPM
    - Klucz poręczenia (Endorsement Key, **EK**), klucz główny magazynu (Storage Root Key, **SRK**), klucze atestacji tożsamości (Attestation Identity Keys, **AIK**)
  - 6 ogólnych typów kluczy
    - Klucze do przechowywania, podpisywania, wiązania, migracji, dziedziczenia (ang. legacy), typu i „authchange" (do zmiany typu uwierzytelniania)
  - Najważniejsze typy kluczy omówiono w kolejnych slajdach
- Każdy klucz może mieć dodatkowe właściwości, najważniejsze to
  - Migrowalne, niemigrowalne, certyfikowane klucze migrowalne (Certified Migration Key, CMK)
    - np. wskazanie, że klucz może być migrowany do innego TPM
  - Oznaczenie, że klucz może być używany tylko wtedy, gdy platforma jest w określonej (potencjalnie bezpiecznej) konfiguracji

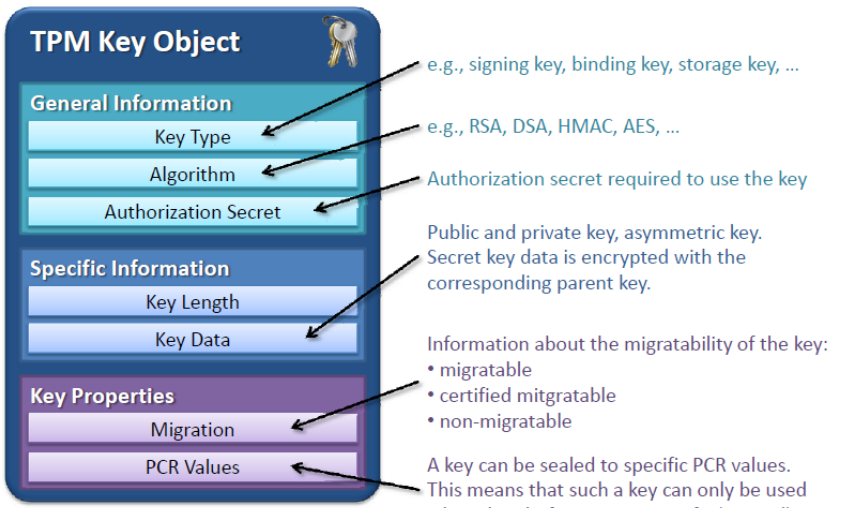
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Obiekt typu klucz (TPM 1.2) – istotne pola

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



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

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Atrybuty kluczy TPM 2.0 [2022-11-18]

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Do każdego klucza (obiektu) przypisane są indywidualne mechanizmy kontroli bezpieczeństwa, które mogą bazować na haśle, zaawansowanych politykach autoryzacji, ograniczeniach dotyczące duplikacji kluczy do innego elementu nadrzędnego lub innego modułu TPM oraz ograniczeniach użycia klucza tylko do podpisywania lub odszyfrowywania.
  - Klucze mogą być zarówno certyfikowane, jak również można ich używać do certyfikacji innych kluczy.
- W TPM 2.0 schemat typów kluczy (stosowany w TPM 1.2) został zastąpiony przypisaniem kluczom trzech podstawowych atrybutów: ***sign***, ***decrypt*** i ***restrict***.
  - Klucze mogą mieć jeden, dwa lub wszystkie trzy atrybuty w dowolnej kombinacji.
  - Do podpisywania danych można używać kluczy z atrybutem **sign**, zaś do odszyfrowania danych kluczy z atrybutem ***decrypt***.
  - Atrybut ***restrict*** powoduje, że klucze działają podobnie do kluczy SRK i AIK w TPM 1.2: klucz z atrybutami ***restrict*** i ***sign*** można użyć do podpisania danych utworzonych tylko przez moduł TPM lub danych użytkownika, których nie można pomylić z danymi TPM, zaś klucz z atrybutami ***restrict*** i ***decrypt*** może być używany tylko jako jedna część w hierarchii magazynu ochrony danych modułu TPM.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

Atrybuty kluczy (TPM 2.0)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Attribute			
restricted	*sign*	*decrypt*	Nominal Usage
0	0	0	External data that is protected (via bind or seal) by the hierarchy
0	0	1	A key for protecting data
0	1	0	A key for signing data
0	1	1	A key for protecting and signing external data
1	0	1	A storage key, for constructing the hierarchy
1	1	0	A key for signing TPM data (certificates, quotes) (an "AK")
1	0	0	Forbidden combination (don't know what it means)
1	1	1	Forbidden combination (it has no useful purpose and is incompatible with the USA's FIPS specifications)

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie — Wydział Informatyki

Atrybuty kluczy TPM 2.0

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Klucze podstawowe, wyprowadzane z ziarna hierarchii kluczy TPM2.0, są tworzone za pomocą polecenia **TPM2_CreatePrimary**.
- Inne klucze i obiekty są tworzone za pomocą polecenia **TPM2_Create**. Należy zauważyć, że w TPM 2.0 klucze i obiekty traktowane są tak samo: klucze to tylko jeden z rodzajów obiektów;
  - to samo polecenie jest używane do tworzenia kluczy asymetrycznych, kluczy symetrycznych, zaszyfrowanych danych i skrótów z kluczem.
- Klucze mogą być duplikowalne (migrowalne w TPM 1.2), a także certyfikowane.
- TPM ma na celu zapewnienie środków do tworzenia hierarchii kluczy magazynu w celu ochrony danych i kluczy (kluczy generowanych przez TPM lub inną jednostkę).
- Każdy z tych obiektów (klucze i dane) ma dwa składniki:
  - **obszar publiczny**, który zawiera atrybuty obiektu i tożsamość publiczną;
  - **obszar wrażliwy** zawierający elementy obiektu wymagające zabezpieczeń TPM; te elementy obejmują wartość autoryzacji, co najmniej jedną wartość klucza tajnego oraz, w niektórych przypadkach, zapieczętowane wartości danych.

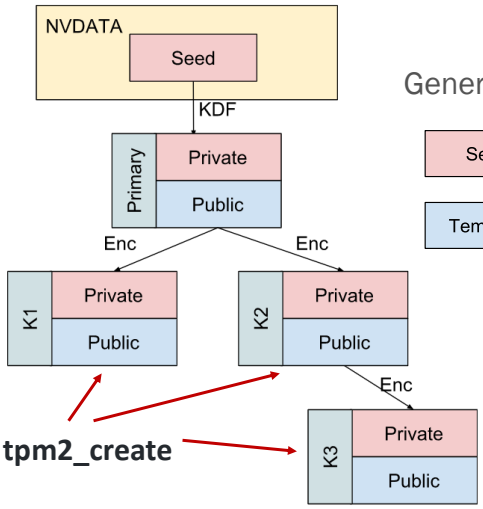
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

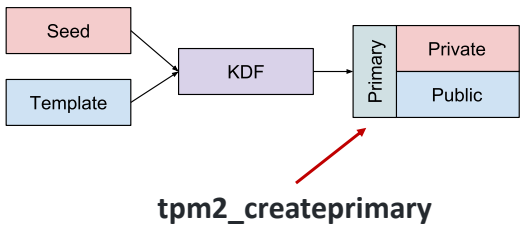
Przykład hierarchii kluczy w TPM 2.0

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Generowanie klucza podstawowego



https://google.github.io/tpm-js/

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Public Area Parameters TPM 2.0 (TPM Library Part 1: Architecture)

Parameter	Description
type	This identifies the type of the object. An algorithm ID is used as the type identifier because the structures contain parameters that are specific to the types of operations that can be performed on or with the object. For example, an RSA type would contain an RSA key pair that could be used for operations defined for RSA. An AES type would be used for symmetric encryption or decryption.
nameAlg	This is a second algorithm ID that identifies the hash algorithm used for computing the Name of the object.
objectAttributes	This contains the set of attributes of the object. These attributes are in five classes: 1) usage (sign, encrypt, restricted); 2) authorization (userWithAuth, adminWithPolicy, noDA); 3) duplication (fixedParent, fixedTPM, encryptedDuplication); 4) creation (sensitiveDataOrigin); and 5) persistence (stClear).
authPolicy	This will contain the authorization policy for the object if one is defined. nameAlg is used as the authPolicy hash algorithm, NOTE An object that is intended to be duplicated must have an authPolicy enabling the duplication.
[type]parameters	The parameters of an object are dependent on the object type. For symmetric key object, the parameters would indicate the size of the key and the default encryption mode. For an asymmetric object (RSA or ECC), the parameters would indicate the key size, signing scheme, and symmetric encryption methods associated with the key.
[type]unique	The unique value of an object is also dependent on the object type. For an asymmetric object, this will be the public key. For a symmetric object, this will be a value computed by hashing values in the sensitive area.

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Sensitive Area Parameters TPM 2.0 (TPM Library Part 1: Architecture)

Parameter	Description
sensitiveType	This identifies the type of the object for this sensitive area. This value and the type parameter of the public area are the same.
authValue	This is the authorization value for the object. It is an octet array of zero or more octets. The authorization value for an object may not have more octets than the digest produced by the object's nameAlg.
seedValue	This value is required for Storage Keys and is the seed used to generate the protection values for the child objects of the Key. This is optional for asymmetric keys that are not Storage Keys and is not used if present. For all other object types, this is an obfuscation value. It is hashed with the sensitive field to produce the unique value in the public area. Including this value in the computation obfuscates unique so that the sensitive value cannot be determined from the unique field.
[sensitiveType] sensitive	The contents of this parameter are dependent on sensitiveType. For an asymmetric key, this will contain the private key. For a symmetric key, this will be the key. For an HMAC key this is the HMAC key value. For a data object, this will be the sensitive data.

Obszar wrażliwy jest powiązany z obszarem publicznym i zawiera dane, które mają być zaszyfrowane, gdy nie znajdują się w chronionej lokalizacji w module TPM.

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Wydział Informatyki
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

Klucz poręczenia platformy (EK)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Klucz poręczenia (ang. Endorsement Key, EK)
  - Generowany przez producenta w bezpiecznym środowisku
    - w TPM lub na zewnątrz TPM, a następnie załadowany do TPM
  - Niemigrowalny, przechowywany wewnątrz układu scalonego, nie może być usunięty
  - Stosowany podczas zdalnej atestacji platformy
- Musi być certyfikowany przez podmiot generujący EK
  - np. przez producenta TPM
- Certyfikat cyfrowy potwierdza, że
  - EK został poprawnie utworzony i osadzony w module TPM
- EK jest głównym punktem zaufania do raportów (RTR) w hierarchii potwierdzeń i służy do poświadczania Attestation Identity Keys (AIK).
- Klucz poręczenia (EK) jednoznacznie określa tożsamość modułu TPM.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Główny klucz magazynu (SRK)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Główny klucz magazynu (ang. Storage Root Key, SRK), 2048 bitowy klucz RSA
  - Jest położony najwyżej w hierarchii kluczy TPM
  - Tworzony podczas przejmowania TPM na własność
    `TPM_TakeOwnership(TPM 1.2)` (TPM 2.0 – patrz dalej)
  - Usuwany wtedy, gdy moduł TPM traci swojego właściciela po wykonaniu operacji `TPM_ForceClear` (TPM 2.0 – patrz dalej)
    - Operacja ta sprawia, że hierarchia kluczy jest niedostępna i tym samym niszczony jest dostęp do wszystkich danych zaszyfrowanych kluczami należącymi do hierarchii
  - Niemigrowalny, przechowywany wewnątrz układu scalonego, może być usunięty

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Przejęcie na własność TPM 1.2

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- TPM jest dostarczany w stanie "unowned"
- Aby poprawnie korzystać z TPM, właściciel platformy musi wykonać operację przejęcia TPM na własność (ang. taking ownership) `TakeOwnership -z`.
  - Ustawienie hasła właściciela – wprowadzenie wspólnego sekretu do TPM (przechowywanego w chronionej lokalizacji)
  - Niektóre operacje TPM wymagają autoryzacji właściciela
  - Fizyczna obecność umożliwia dostęp do pewnych (inaczej chronionych przez właściciela) funkcjonalności TPM; obecność ta nie ujawnia żadnych sekretów TPM (np. hasła właściciela)
  - `ForceClear` pozwala na zablokowanie operacji TPM wymagających fizycznej obecności
- Generowanie SRK jest częścią realizacji operacji `TakeOwnership`
- (Prywatny) klucz SRK jest przechowywany wewnątrz TPM i nigdy go nie opuszcza
- Użycie SRK może wymagać podania hasła

Przejęcie na własność TPM 2.0 i jego anulowanie

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Przejęcie na własność modułu TPM 2.0 polega na zdefiniowaniu wartości autoryzacji (*authValue*) dla *ownerAuth*, *endorsementAuth* i *lockoutAuth*.
  - TMP 2.0 po wykonaniu trzech nieudanych prób dostępu do obiektu blokuje się; odblokowanie wymaga pomyślnej autoryzacji zgodnej z wartością *lockoutAuth*.
- Specyfikacja TPM Library Part 1: Architecture nie zawiera definicji polecenia `TakeOwnership`. Polecenie to jest jednak dostępne w wielu dystrybucjach systemu Linux, np. Suse, Ubuntu, Debian:

  Przykład: `tpm2_takeownership -o ownerpass -e endorsepass -l lockpass`

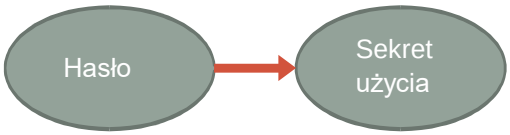
- Operacja rezygnacji z prawa własności usuwa aktualnego właściciela z modułu TPM. Służy do tego polecenie TPM2_Clear, które m.in.:
  - usuwa wszelkie przejściowe lub trwałe obiekty związane z hierarchiami SPS (Storage Primary Seed) lub EPS (Endorsement Primary Seed); nie ma to wpływu na obiekty PPS (Platform Primary Seed);
  - zastępuje istniejący SPS nową wartością z generatora RNG.

Hasła i sekrety

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Podczas przejmowania TPM na własność ustawiany jest sekret (TPM 1.2) lub sekrety właściciela, które są potrzebne później podczas konieczności wykonania niektórych poleceń TPM.
- Dane autoryzacyjne związane są także z każdym chronionym obiektem, np. kluczem; należy go przedstawić zawsze wtedy, gdy konieczne jest wykonanie określonej operacji z użyciem chronionego obiektu (za sekret pozwalający na użycie EK można można uznać dane autorryzacyjne właściciela TPM).
- Z wartości autoryzacyjnej może być wyprowadzony sekret, który można używać np. w operacjach kryptograficznych lub protokołach autoryzacji.



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

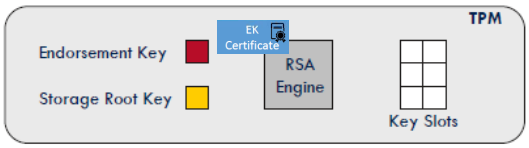
Wydział Informatyki

Klucze EK i SRK w TPM

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- EK i SRK są jedynymi kluczami na trwałe przechowywanymi wewnątrz TPM
  - W TPM 2.0 trwałość kluczy odnosi się kluczy podstawowych związanych z hierarchią kluczy: hierarchia magazynu (SRK i AIK), hierarchia poręczenia (EK). Trwałe mogą być także klucze inne niż klucze podstawowe ulokowane w hierarchii poręczenia, magazynu i platformy
- Użycie klucza nietrwałego wymaga załadowania go do TPM
- Zarządzanie slotami kluczy jest realizowane programowo - Trusted Software Stack (TSS)



- Aby utworzyć parę kluczy umieszczane w hierarchii kluczy, należy wskazać klucz rodzica.

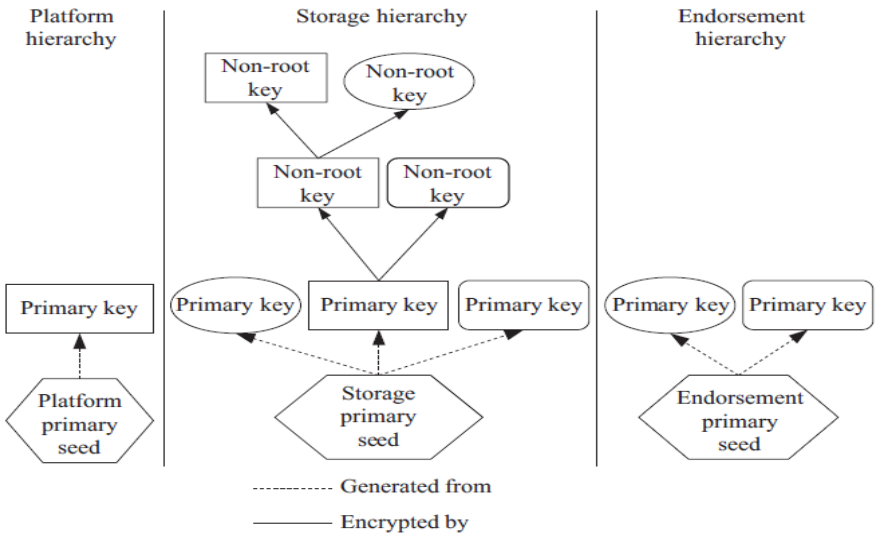
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Klucze PK, EK i SRK w TPM 2.0

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

61

Klucze magazynowania (StorK)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Przenaczenie kluczy StorK (klucze do przechowywania kluczy): ochrona kluczy poza TPM
  - np. klucz magazynowania może służyć do szyfrowania innych kluczy, które mogą być przechowywane na dysku twardym
  - główny klucz magazynu (SRK) jest specjalnym kluczem magazynowania
  - ochrona konfiguracja/właściwości systemu (pieczętowanie, ang. sealing)
    - np. szyfrowanie sekretów, które można odzyskać tylko wtedy, gdy platforma ma odpowiednio zdefiniowane środowisko sprzętowo-programowe
- Własności
  - Zazwyczaj 2048-bitowa para kluczy szyfrowania/deszyfrowania RSA
  - Zasadniczo można migrować je do innych modułów TPM
    - nie mogą być kluczami niemigrowalnymi, jeśli jeden z kluczy rodziców podlega migracji
    - nie mogą być migrowalne, jeśli klucze są używane do **pieczętowania**

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

62

Klucze atestacji tożsamości (AIK)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Przeznaczenie
  - Stosowane do atestacji aktualnej konfiguracji platformy
  - Dowiązanie tożsamości do TPM/platformy (do Endorsement Key)
  - Stosowanie kluczy AIK powinno zapobiec śledzeniu TPM-ów i/lub platform obliczeniowych.
- Własności
  - Klucze AIK są niemigrowalnmi kluczami podpisującymi
  - Generowane przez właściciela TPM
  - TPM/platforma może mieć wiele kluczy AIK

Certyfikacja kluczy AIK

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- AIK wymaga certyfikacji kluczy AIK wygenerowanych przez TPM.
- Specyfikacje TCG dopuszczają dwie możliwości
  - Certyfikacja przez Trusted Third Party (Privacy CA wg terminologii TCG), która poświadcza, że klucz AIK został wygenerowany przez określony TPM
    - Problem prywatności: Privacy CA pozwala na powiązanie transakcji z konkretnym TPM.
  - Certyfikacja poprzez DAA (Direct Anonymous Attestation)
    - Umożliwia uzyskanie niepowiązalności (ang. unlinkability) transakcji z TPM
    - Nie jest wymagany urząd CA
    - Pozwala na użycie dowodu wiedzy zerowej (Zero Knowledge Proof, ZKP) posiadania ważnego certyfikatu (bez ujawniania samego certyfikatu)

Klucze wiązania (ang. binding keys)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Przeznaczenie
  - Ochrona dowolnych danych znajdujących się poza TPM
    - Wiązanie jest równoważne tradycyjnemu szyfrowaniu asymetrycznemu
- Własności
  - Jest to zazwyczaj para kluczy szyfrowania/deszyfrowania RSA o długości 2048 bitów
    - moduł TPM może obsługiwać także inne schematy szyfrowania asymetrycznego
  - Klucze wiązania można używać tylko w operacjach wiązania
  - Możliwość migracji na inne TPM/platformy
    - Niedozwolone jest, aby klucze nie podlegały migracji, jeśli jeden z kluczy nadrzędnych (kluczy rodzica) podlega migracji.

Wiązanie a pieczętowanie (binding vs. sealing)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Wiązanie

- Tradycyjne szyfrowanie asymetryczne
- Może być użyte do wiązania danych z konkretnym TPM
  - Dane zaszyfrowane za pomocą niemigrowalnego klucza mogą być odtworzone tylko przez ten TPM, który zna odpowiedni klucz sekretny.
- Zwykle brak wiązania z platformą
  - .. ponieważ wiązanie można budować także z użyciem kluczy migrowalnych
- Nie wymaga interakcji z TPM

Pieczętowanie (rozszerzenie wiązania)

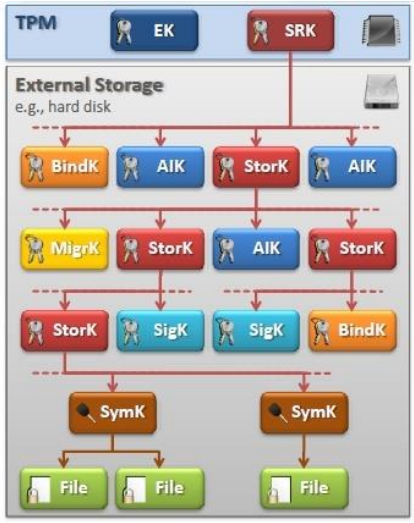
- Pozwala na związanie danych z konkretną platformą TPM
  - Pieczętowanie można stosować tylko z kluczami niemigrowalnymi
- Można zweryfikować konfigurację platformy szyfrowania
  - Szyfrogram zawiera stan platformy w momencie szyfrowania
- Można wiązać dane z konkretną konfiguracją platformy
  - Dane można odszyfrować tylko wtedy, gdy platforma jest w predefiniowanym (prawdopodobnie zaufanym) stanie

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

Drzewo hierarchii kluczy TPM 1.2

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



- Z każdym kluczem związane są 160-bitowe dane uwierzytelniające *authData*.
- Liczba poziomów hierarchii oraz liczba kluczy chronionych przez TPM jest ograniczona tylko rozmiarem pamięci nośnika zewnętrznego.
- Klucze magazynów (StorK) chronią pozostałe typy kluczy (liście w drzewie hierarchii)
  - Attestation Identity Keys (AIK)
  - Signing keys (SigK)
  - Binding Keys (BindK)
  - Migration Keys (MigrK)
  - Symmetric Keys (SymK)
- SRK pośrednio chroni dowolne dane (np. pliki)

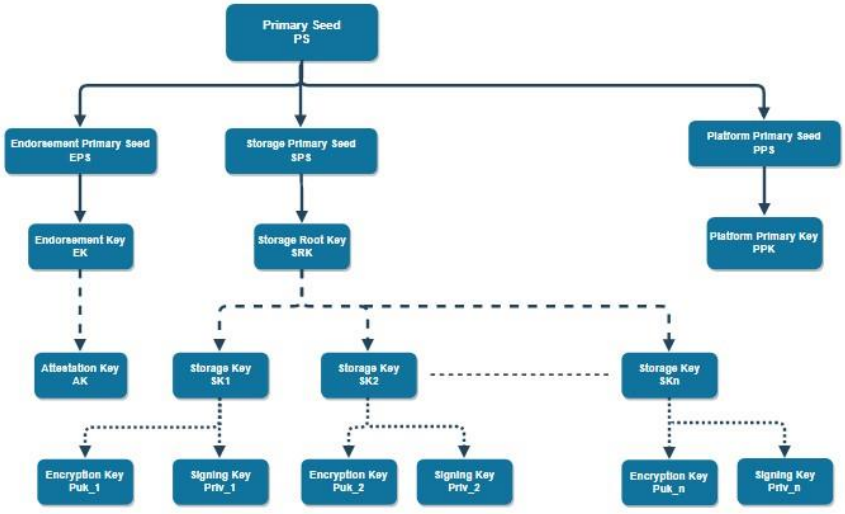
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Drzewo hierarchii kluczy TPM 2.0

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Hierarchia kluczy TPM

INFORMACJE ...

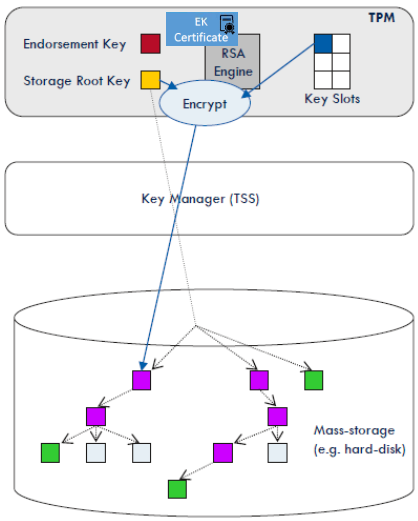
- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Po przemieszczeniu kluczy poza TPM ustanawiana jest ich hierarchia
- Ilekroć klucz jest eksportowany z TPM, to jego część prywatna jest szyfrowana za pomocą klucza publicznego rodzica
- Wg terminologii TCG klucz potomka jest opakowywany (szyfrowany) za pomocą klucza prywatnego magazynu
- Ponieważ klucze prywatne rodziców (wymagane podczas ładowania/deszyfrowania klucza potomka) nigdy nie opuszczają TPM w postaci jawnej, to klucz prywatny TPM nigdy nie może być deszyfrowany/używany poza TPM
- Klucz prywatny SRK, ulokowany na szczycie hierarchii kluczy, nigdy nie jest eksportowany poza TPM
- Klucze magazynu tworzą węzły hierarchii kluczy, podczas gdy klucze podpisujące/szyfrujące są zawsze liśćmi

Wypakowywanie kluczy z TPM

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

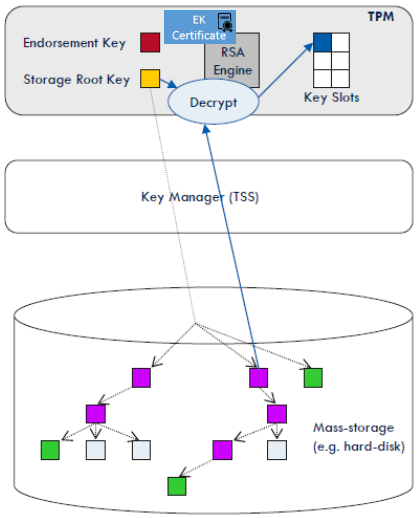


- Hierarchia kluczy z SRK jako korzeniem (ang. root)
- Prywatny klucz SRK nigdy nie opuszcza TPM
- Eksportowanie klucza w formacie *blob* z TPM
- Klucze prywatne są szyfrowane za pomocą klucza publicznego rodzica zanim klucz w formacie *blob* opuści TPM

Ładowanie kluczy do TPM

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



- Załadowanie klucza podpisującego/deszyfrującego do TPM przed jego użyciem podczas operacji podpisu/deszyfrowania
- Ustanowienie pełnej ścieżki kluczy aż do SRK
- Odszyfrowanie klucza prywatnego wchodzącego w skład klucza magazynu za pomocą klucza prywatnego SRK
- Żądanie użycia sekretu chroniącego SRK

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

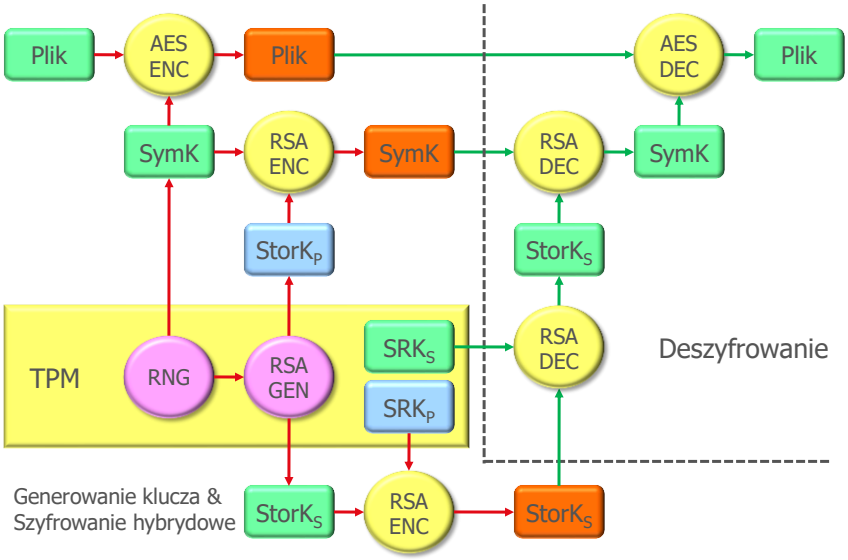
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

71

Hybrydowe szyfrowanie plików za pomocą klucza nośnika [2022-11-24]

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

72

Rejestry PCR

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Pomiar integralności
  - Proces uzyskiwania metryki cech platformy, które wpływają na integralność (wiarygodność) platformy oraz przechowywania wartości skrótów z tych metryk w PCR modułu TPM
  - Metryka cechy platformy = wartość skrótu z oprogramowania, które będzie wykonywane
- Platform Configuration Registers (PCR)
  - Chroniona lokalizacja, w której przechowywane są wartości pomiarów integralności
  - PCR-y mogą być tylko rozszerzane: $PCR_{i+1} \leftarrow \text{Hash}(PCR_i, value)$
  - Rejestry PCR są resetowane tylko po ponownym uruchomieniu systemu
- Rejestrowanie integralności
  - Przechowywanie metryk integralności w dzienniku zdarzeń w celu późniejszego wykorzystania
  - Zapisywanie dodatkowych informacji o tym, co zostało zmierzone, m.in. nazwa producenta oprogramowania, nazwa, i wersja oprogramowania

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Rejestry PCR – ochrona dzienników zdarzeń

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Rejestry PCR są wykorzystywane do weryfikacji zawartości dziennika pomiarów
- Nominalne zachowanie zaufanej platformy polega na utrzymywaniu w dzienniku zapisów zdarzeń, które wpływają na stan bezpieczeństwa platformy, przynajmniej w trakcie procesu rozruchu i ustanawiania TCB.
- Po uzupełnieniu dziennika moduł TPM otrzymuje kopię wpisu dziennika lub skrót danych zapisanych w dzienniku.
- Dane wysyłane do TPM są zawarte w skumulowanym skrócie w PCR.
- TPM może następnie dostarczyć poświadczenie wartości w PCR, które z kolei weryfikuje zawartość dziennika.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

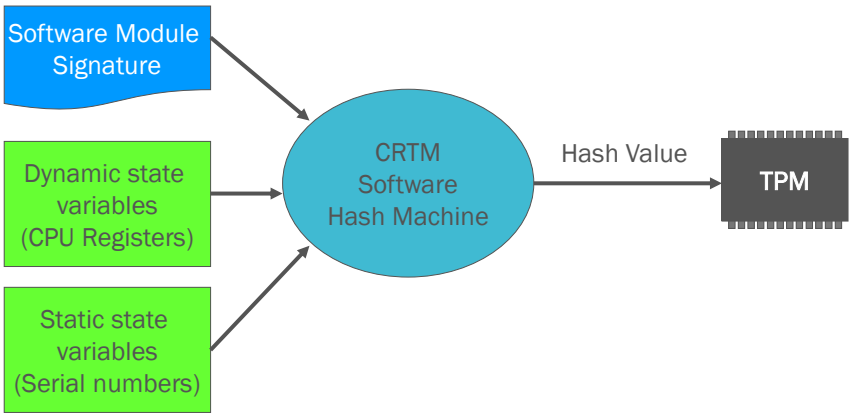
Wydział Informatyki

Rejestry PCR – pomiar integralności

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Hipotetyczny przykład pomiaru integralności



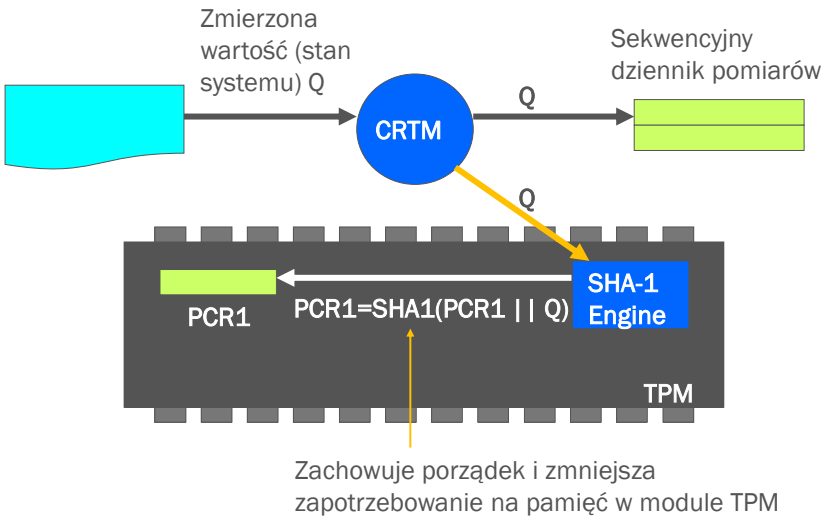
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Rejestry PCR (TPM 1.2) – pomiar integralności

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

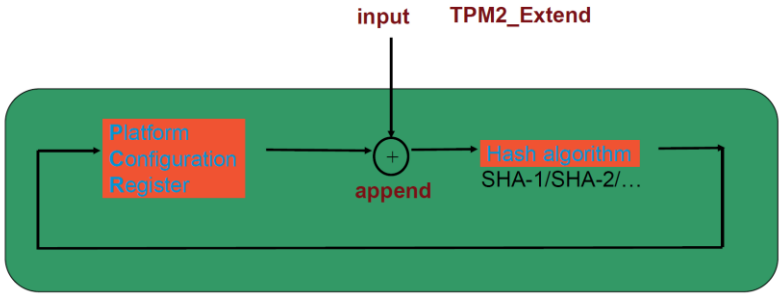
Rejestry PCR (TPM 2.0) – pomiar integralności

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

$$PCR.digest_{new}[pcrNum][alg] := \mathbf{Hash}_{alg}(PCR.digest_{old}[pcrNum][alg] \,\|\, data[alg].buffer)$$

$Hash_{alg}$	funkcja skrótu obliczająca skrót z konkatenacji wartości określonego egzemplarza PCR i nowym skrótem
PCR.digest	wartość skrótu w PCR
pcrNum	numeryczny selektor PCR (prcHandle)
alg	algorytmiczny selektor algorytmu funkcji skrótu związanego z PCR
data[*alg*].*buffer*	specyficzne dla banku dane, o które ma zostać rozszerzony PCR



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Rejestry PCR (TPM 2.0) – pomiar integralności

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- TPM może utrzymywać wiele banków PCR. Bank PCR jest podzbiorem rejestrów PCR, które są rozszerzone za pomocą tego samego algorytmu skrótu. Banki PCR są identyfikowane przez algorytm skrótu używany do rozszerzania PCR w tym banku.
  - Przykład: do jednego banku mogą wchodzić PCR 1, 2, 4 i 5, zaś do innego PCR 1, 2, 3, 9 i 11.
- Banki PCR są rozszerzane oddzielnie
  - Przykład: można rozszerzyć PCR 0 w banku SHA-1 o skrót SHA-1, ale PCR 0 w banku SHA-256 pozostaje bez zmian.
- Każdy bank używa schematu numerowania rejestrów opartego na indeksach, przy czym z tym samym indeksem będą zawsze związane takie same uprawnienia i możliwości kontroli dostępu, niezależnie od banku.
  - Przykład: PCR 17 w banku SHA-1 i PCR 17 w banku SHA-256 będą miały te same właściwości resetowalności, te same ograniczenia rozszerzalności i taką samą politykę autoryzacji lub hasło.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Rejestry PCR (TPM 2.0) – pomiar integralności

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- Polecenie **TPM2_PCR_Extend** pobiera listę oznaczonych skrótów, na której każdy wpis zawiera indeks PCR i nazwę banku.

  tpm2_pcrextend **4:sha1**=f1d2d2f924e986ac86fdf7b36c94bcdf32beec15,
  7:sha256=b5bb9d8014a0f9b1d61e21e796d78dccdf1352f23cd32812f4850b878ae4944c
  - Polecenie można wykorzystać do rozszerzenia wielu banków o równoważne skróty utworzone przy użyciu różnych funkcji skrótu, a także do rozszerzenia jednym poleceniem wielu PCR należących do tego samego banku.
- Alternatywą dla polecenia **TPM2_PCR_Extend** jest polecenie **TPM2_PCR_Event** (tylko TPM 2.0).Tam, gdzie **TPM2_PCR_Extend** pobiera wstępnie obliczony skrót, polecenie **TPM2_PCR_ Event** pobiera dane (do 1024 bajtów) i indeks PCR. Moduł TPM oblicza niezbędne skróty, a następnie rozszerza wartość tego PCR we wszystkich dostępnych bankach.
  - Jeśli korzystamy z wielu banków PCR, to używanie polecenia TPM2_PCR_Event jako standardowego mechanizmu rozszerzania PCR jest dobrą praktyką, ponieważ zminimalizuje ryzyko utraty synchronizacji banków.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Rejestry PCR (TPM 2.0) – pomiar integralności

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

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Initial state, PCR 1 [SHA1 bank]

0000000000000000000000000000000000000000

Initial state, PCR 1 [SHA256 bank]

0000000000000000000000000000000000000000000000000000000000000000

TPM2_PCR_EVENT(1, "foo")

SHA-1(0000000000000000000000000000000000000000 | SHA-1("foo"))

SHA-256(0000000000000000000000000000000000000000000000000000000000000000 | SHA-256("foo"))

New state, PCR 1 [SHA1 bank]

57c67daaf488d6a6e627214d256b15c5accdb437

New state, PCR 1 [SHA256 bank]

13e8bb57756e58d8e81f69df782e79944feed675697cffc1fcd23019331fcb25

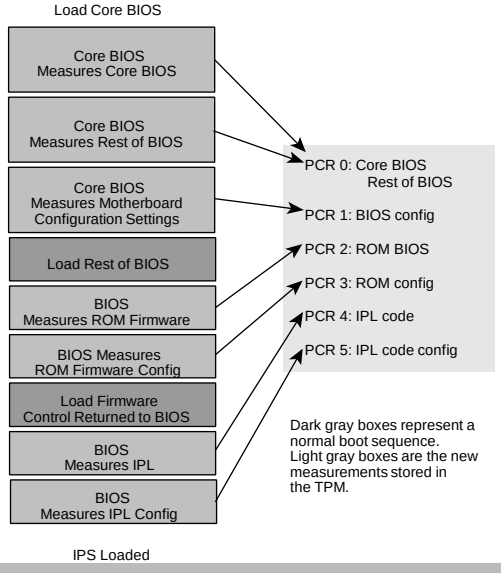
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Rejestry PCR – pomiar integralności BIOS

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

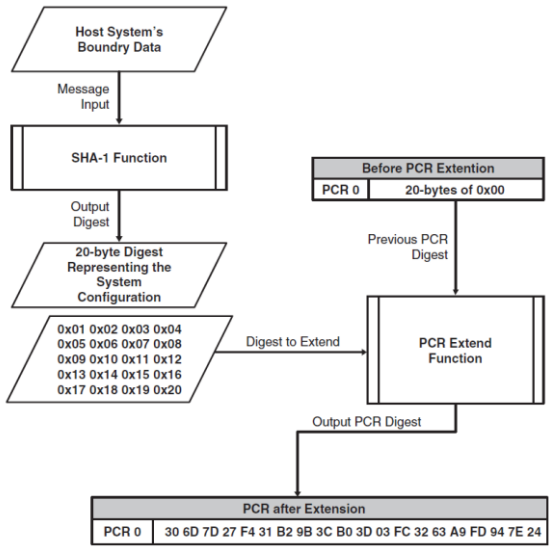
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

81

Rejestry PCR – rozszerzanie rejestru

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

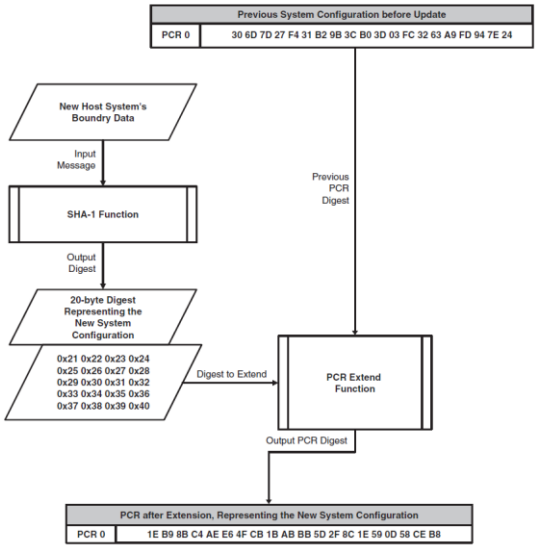
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

82

Rejestry PCR – rozszerzanie rejestru odzwierciedlające aktualizację systemu

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

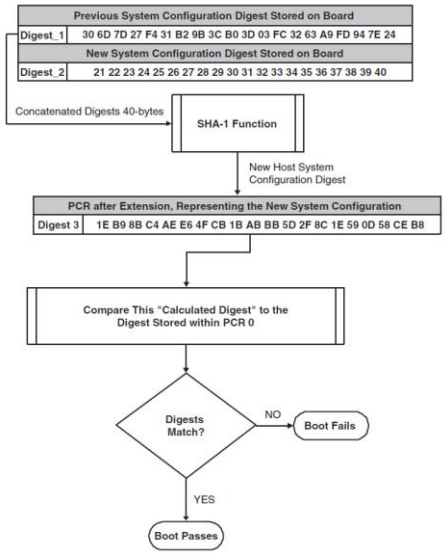
ZAUFANA INFRASTRUKTURA OBLICZENIOWA

83

Rejestry PCR – testowanie nowej konfiguracji uruchamiającej system

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

ZAUFANA INFRASTRUKTURA OBLICZENIOWA

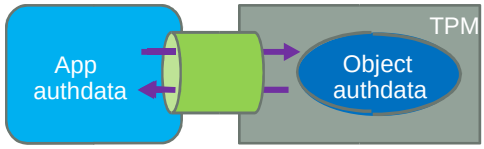
84

Sesje TPM – protokoły autoryzacji

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

- W celu ochrony komunikacji między aplikacją a TPM większość poleceń wspieranych jest przez mechanizmy ochronne.
  - Wykorzystywane są dane autryzujące *authdata* (authValue lub authPolicy w TPM 2.0) obiektu.
- Ponieważ interakcja aplikacji z modułem TPM może wymagać sekwencji kilku poleceń, stąd grupowane są one w sesje obsługiwane przez moduł TPM.



- TPM1.2 obsługuje dwa różne typy sesji
  - **OIAP**: Object Independent Authorization Protocol tworzy sesję, która pozwala manipulować dowolnym obiektem, ale wymaga, aby dane autoryzacyjne były prezentowane dla każdego polecenia.
  - **OSAP**: Object Specific Authorization Protocol tworzy sesję, która pozwala manipulować określonym obiektem wskazanym podczas inicjowania sesji. Dane autoryzacyjne muszą być prezentowane tylko raz i mogą być używane wielokrotnie, o ile tylko ten obiekt (taki jak klucz lub obiekt blob) jest dostępny. Każdy używany obiekt wymaga odrębnej sesji autoryzacji.

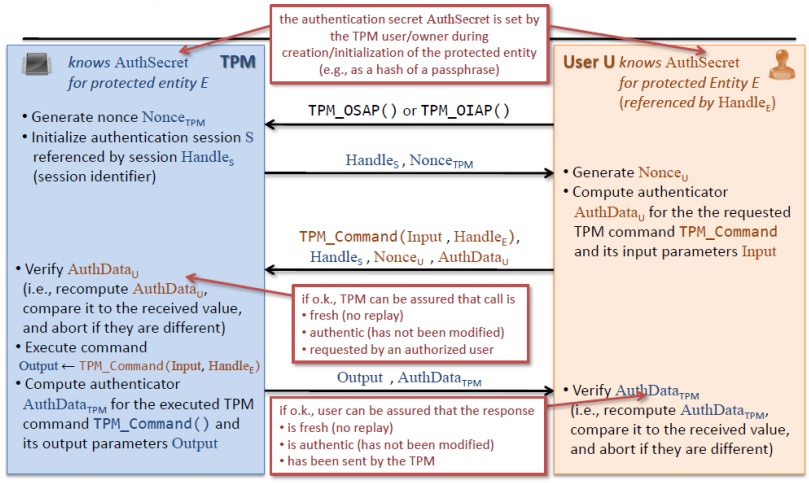
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Podstawowa funkcjonalność protokołu uwierzytelniania TPM 1.2

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



$AuthData_U \leftarrow HMAC(AuthSecret ; SHA\text{-}1(TPM\_Command , Input) , Nonce_{TPM} , Nonce_U)$

$AuthData_{TPM} \leftarrow HMAC(AuthSecret ; SHA\text{-}1(TPM\_Command , Output) , Nonce_U)$

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

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

OIAP vs OSAP (TPM 1.2)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

OIAP (Object Independent Authentication Protocol)

- Właściwości
  - Pozwala na autoryzowanie dostępu do wielu różnych chronionych jednostek za pomocą wielu poleceń
  - Do autoryzacji wielu różnych jednostek niezbędna jest tylko jedna konfiguracja
  - Brak ustanowienia klucza sesji
- Głównie stosowany do
  - Autoryzacji korzystania z chronionych jednostek bez potrzeby posiadania wspólnego sekretu/klucza sesji

OSAP (Object Specific Authentication Protocol)

- Właściwości
  - Pozwala na autoryzowanie dostępu do jednej chronionej jednostki za pomocą wielu poleceń
  - Do autoryzacji każdej jednostki wymagana jest oddzielana konfiguracja
  - Ustanawiany jest efemeryczny wspólny klucz sesji, który może być używany jako klucz kryptograficzny
- Głównie stosowany do
  - Ustawienia lub zmiany danych uwierzytelniających związanych z chronionymi jednostkami

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

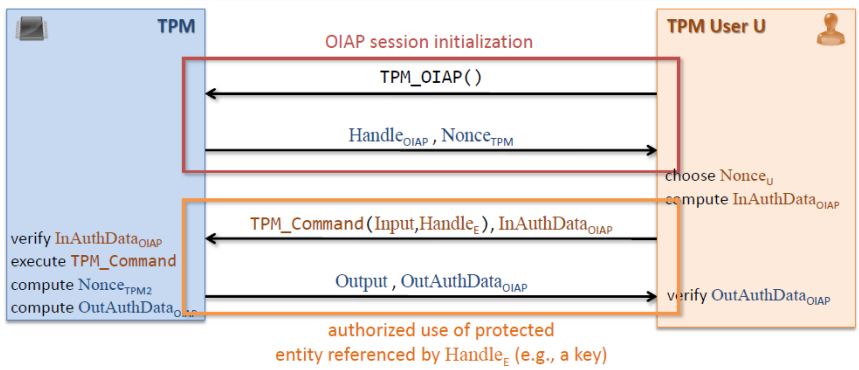
Protokół OIAP (TPM 1.2)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki



User Authentication data: $InAuthData_{OIAP} \leftarrow (Handle_{OIAP} , Nonce_U , InAuthDigest_{OIAP})$

Authenticator of user U: $Digest_{OIAP} \leftarrow HMAC(AuthSecret_{Entity} ; SHA\text{-}1(TPM\_Command , Input) , Nonce_{TPM} , Nonce_U)$

InAuth

TPM Authentication data: $OutAuthData_{OIAP} \leftarrow (Nonce_{TPM,2} , OutAuthDigest_{OIAP})$

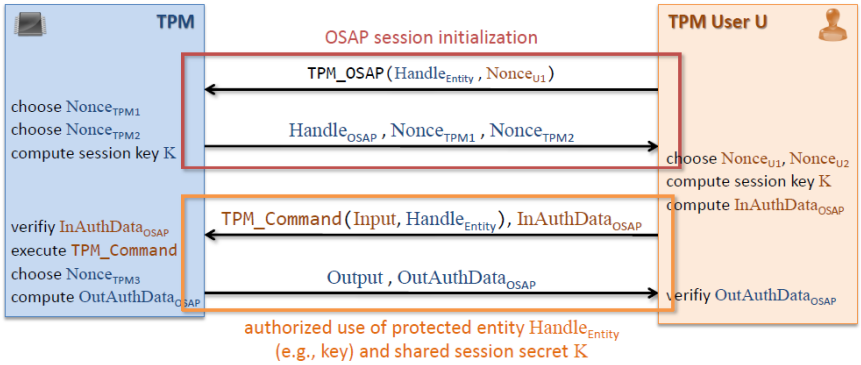
Authenticator of TPM: $OutAuthDigest_{OIAP} \leftarrow HMAC(AuthSecret_{Entity}; SHA\text{-}1(TPM\_Command, Ouput), Nonce_{TPM2}, Nonce_U)$

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

Protokół OSAP (TPM 1.2)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Session key: $K \leftarrow HMAC(\ AuthSecret_{Entity}\ ,\ Nonce_{TPM2}\ ,\ Nonce_{U1}\ )$

User authentication data: $InAuthData_{OSAP} \leftarrow (\ Handle_{OSAP}\ ,\ Nonce_{U2}\ ,\ InAuthDigest_{OSAP}\ )$

Authenticator of user U: $InAuthDigest_{OSAP} \leftarrow HMAC(\ K\ ,\ SHA\text{-}1(\ TPM\_Command\ ,\ Input\ )\ ,\ Nonce_{TPM1}\ ,\ Nonce_{U2}\ )$

TPM authentication data: $OutAuthData_{OSAP} \leftarrow (\ Nonce_{TPM3}\ ,\ OutAuthDigest_{OSAP}\ )$

Authenticator of TPM: $OutAuthDigest_{OSAP} \leftarrow HMAC(\ K\ ,\ SHA\text{-}1(\ TPM\_Command\ ,\ Ouput\ )\ ,\ Nonce_{TPM3}\ ,\ Nonce_{U2}\ )$

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

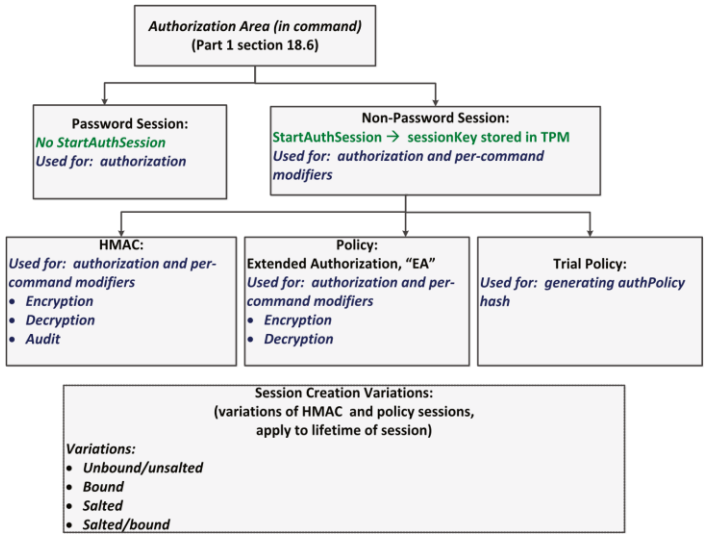
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Sesje TPM 2. 0

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Sesje TPM 2. 0

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Sesja to zbiór stanów TPM, które zmieniają się po każdym użyciu tej sesji. Sesja ma trzy zastosowania:

1) **Autoryzacja** - sesja związana z uchwytem i służy do autoryzacji użycia obiektu powiązanego z tym uchwytem.
2) **Audyt** – w ramach sesji audytu zbierane są skróty parametrów polecenia/odpowiedzi, które są dowodem wystąpienia określonej sekwencji zdarzeń.
3) **Szyfrowanie** - sesja, która nie jest używana do autoryzacji lub audytu, ale może być konieczna podczas wykonywania polecenia szyfrowania lub zwracania paramertów odpowiedzi.

Dalej skupimy się tylko na sesjach autoryzacji. Zarówno sesje autoryzacji oparte na HMAC, jak i sesje autoryzacji oparte na politykach są inicjowane za pomocą polecenia **TPM2_StartAuthSession**. Parametry tego polecenia mogą zostać tak wybrane, aby zostały utworzone różne sesji.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Sesje TPM 2. 0 – protokoły autoryzacji

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Rozważymy sesje autoryzacji oparte na HMAC (*sessionType* = HMAC). Moduł TPM 2.0 zapewnia cztery rodzaje sesji HMAC w zależności od różnych kombinacji parametrów *tpmkey* i *bind,* ustawianych podczas tworzenia sesji:

1) **Sesja niepowiązana i bez ziarna** (ang. unbound and unsalted session). W tej wersji sesji *tpmkey* i *bind* mają wartość NULL.
2) **Sesja powiązana** (ang. bound session). W tym typie sesji *tpmkey* jest równe NULL, ale *bind* jest różne od NULL i wskazuje na jakąś jednostkę TPM z wartością *authValue wykorzystywaną* podczas generowania klucza sesji *sessionKey*.
3) **Sesja z ziarnem** (ang. salted session) . W przypadku tego typu sesji *bind* ma wartość NULL, ale obecny jest *tpmkey*, wskazujący na klucz używany do szyfrowania wartości ziarna; to daje możliwość uwzględnienia dodatkowej entropii (ziarna) podczas generowania klucza sesji.
4) **Sesja z ziarnem i pozwiązana** (ang. salted and bound session). W tej sesji występuje zarówno *bind*, jak również *tpmkey.* Powiązanie służy do dostarczania wartości *authValue*, z kolei *tpmkey* szyfruje wartość ziarna, a *sessionKey* jest obliczany przy użyciu obu z nich.

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM 2.0 HMAC authorization

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

F. Yu, et. al. *A formal analysis of Trusted Platform Module 2.0 hash-based message authentication code authorization under digital rights management scenario*, **Security and Communication Networks, Volume: 9, Issue: 15, Pages: 2802-2815, First published: 23 January**

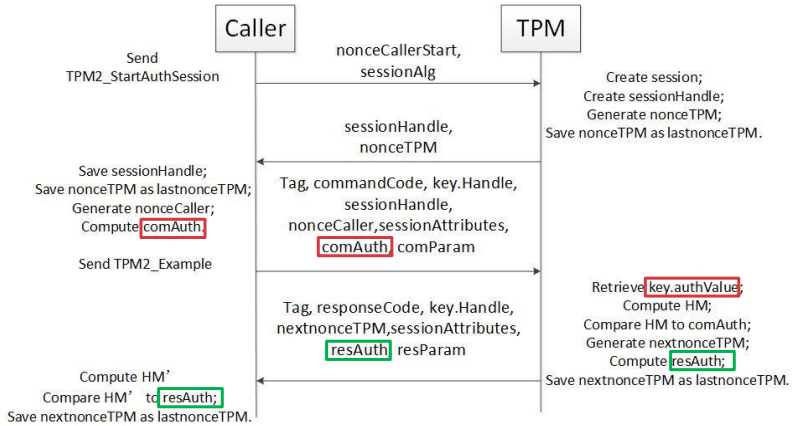
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Protocol based on Unbound and Unsalted HMAC Session (w TPM 2.0, TPM Library, part 1) → protokół OIAP (TPM 1.2)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



$comAuth = HMAC_{sessionAlg}(key.authValue, (cpHash||nonceCaller||lastnonceTPM||sessionAttributes))$

$resAuth = HMAC_{sessionAlg}(key.authValue, (rpHash||nextnonceTPM||nonceCaller||sessionAttributes))$,

W. Wang, Yu Qin, D. Feng, X. Chu Automated Proof for Authorization Protocols of TPM 2.0 in Computational Model

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Protocol based on Unbound and Unsalted HMAC Session (w TPM 2.0, TPM Library, part 1) → protokół OIAP: porównanie

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

TPM 2.0

comAuth=$HMAC_{sessionAlg}$(*key.authValue*,(*cpHash*||*nonceCaller*||*lastnonceTPM*||*sessionAttributes*))

resAuth =$HMAC_{sessionAlg}$(*key.authValue*, (*rpHash*||*nextnonceTPM*||*nonceCaller*||*sessionAttributes*)),

cpHash = $H_{sessionAlg}$(commandCode || key.name || comParam)

rpHash = $H_{sessionAlg}$(responseCode || commandCode || resParam)

TPM 1.2

User Authentication data: $InAuthData_{OIAP} \leftarrow (\ Handle_{OIAP}\ ,\ Nonce_{U}\ ,\ InAuthDigest_{OIAP}\ )$

Authenticator of user U: $Digest_{OIAP} \leftarrow HMAC(\ AuthSecret_{Entity}\ ;\ SHA\text{-}1(TPM\_Command\ ,\ Input)\ ,\ Nonce_{TPM}\ ,\ Nonce_{U}\ )$

InAuth

TPM Authentication data: $OutAuthData_{OIAP} \leftarrow (\ Nonce_{TPM,2}\ ,\ OutAuthDigest_{OIAP}\ )$

Authenticator of TPM: $OutAuthDigest_{OIAP} \leftarrow HMAC(AuthSecret_{Entity};\ SHA\text{-}1(TPM\_Command,\ Ouput\ ),\ Nonce_{TPM2},\ Nonce_{U}\ )$

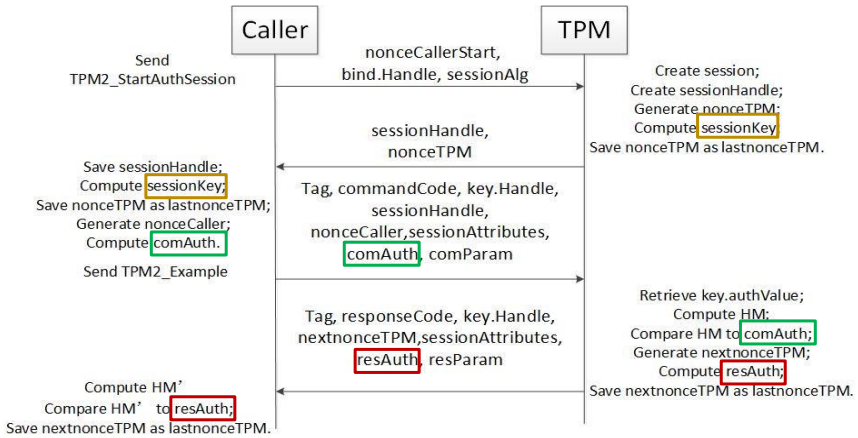
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Protocol based on Bound HAMAC Session (w TPM 2.0, TPM Library, part 1) → protokół OSAP (TPM 1.2)

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania



sessionKey = **KDFa**(*sessionAlg*, *bind.authValue*, "ATH", *nonceTPM*, *nonceCallerStart*, *bits*)

comAuth=**HMAC**$_{sessionAlg}$(*sessionKey*, (*cpHash*||*nonceCaller*||*lastnonceTPM*||*sessionAttributes*))

resAuth =**HMAC**$_{sessionAlg}$(*sessionKey*, (*rpHash*||*nextnonceTPM*||*nonceCaller*||*sessionAttributes*))

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Protocol based on Bound HAMAC Session (w TPM 2.0, TPM Library, part 1) → protokół OSAP (TPM 1.2) - porównanie

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

TPM 2.0

sessionKey = **KDFa**(*sessionAlg, bind.authValue,* "ATH", *nonceTPM, nonceCallerStart, bits*)

comAuth=**HMAC**$_{sessionAlg}$(*sessionKey,* (*cpHash*||*nonceCaller*||*lastnonceTPM*||*sessionAttributes*))

resAuth =**HMAC**$_{sessionAlg}$(*sessionKey,* (*rpHash*||*nextnonceTPM*||*nonceCaller*||*sessionAttributes*))

cpHash = H$_{sessionAlg}$(commandCode || key.name || comParam)

rpHash = H$_{sessionAlg}$(responseCode || commandCode || resParam)

TPM 1.2

Session key: $K \leftarrow HMAC(\ AuthSecret_{Entity}\ ,\ Nonce_{TPM2}\ ,\ Nonce_{U1}\ )$

User authentication data: $InAuthData_{OSAP} \leftarrow (\ Handle_{OSAP}\ ,\ Nonce_{U2}\ ,\ InAuthDigest_{OSAP}\ )$

Authenticator of user U: $InAuthDigest_{OSAP} \leftarrow HMAC(\ K\ ,\ SHA\text{-}1(\ TPM\_Command\ ,\ Input\ )\ ,\ Nonce_{TPM1}\ ,\ Nonce_{U2}\ )$

TPM authentication data: $OutAuthData_{OSAP} \leftarrow (\ Nonce_{TPM3}\ ,\ OutAuthDigest_{OSAP}\ )$

Authenticator of TPM: $OutAuthDigest_{OSAP} \leftarrow HMAC(\ K\ ,\ SHA\text{-}1(\ TPM\_Command\ ,\ Ouput\ )\ ,\ Nonce_{TPM3}\ ,\ Nonce_{U2}\ )$

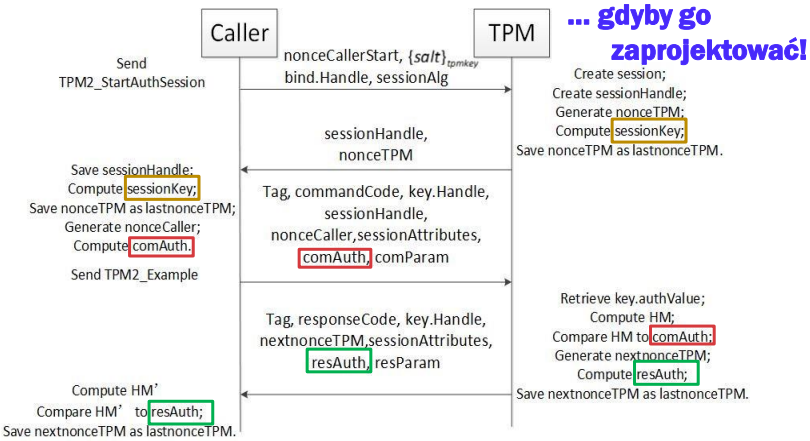
Protocol based on Salted and Bound HAMAC Session (w TPM 2.0, TPM Library, part 1 = **protokół OSAP (TPM 1.2) z ziarnem, ... gdyby go zaprojektować!**

INFORMACJE ...

- Moduł TPM: specyfikacje, rozwój, właściwości, zastosowania
- Zadania TPM i jego główne elementy
- Bezpieczne uruchamianie system
- Tożsamość i klucze
- Rejestry PCR
- Podstawowe protokoły uwierzytelniania

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki



sessionKey = **KDFa**(*sessionAlg, bind.authValue*||*salt*, "ATH", *nonceTPM, nonceCallerStart, bits*)

comAuth=**HMAC**$_{sessionAlg}$(*sessionKey,* (*cpHash*||*nonceCaller*||*lastnonceTPM*||*sessionAttributes*))

resAuth =**HMAC**$_{sessionAlg}$(*sessionKey,* (*rpHash*||*nextnonceTPM*||*nonceCaller*||*sessionAttributes*))

Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

IR EXCELLENCE IN RESEARCH

Wydział Informatyki

DZIĘKUJĘ ZA UWAGĘ

99