

TC

Trusted Computing?
Trustworthy Computing?
Or Trecherous Computing?

Plan

- Wstęp – wizja systemu
- Rys historyczny
- Ogólne założenia
- Jak to działa – warunki sprzętowe i oprogramowania
- Możliwości nadużyć
- Przyszłość TC

O co chodzi?

- TGC – Trusted Computing Group – Microsoft, Intel, AMD, HP, IBM
- Nowa definicja pojęcia „bezpieczeństwo”
- Zamieszanie z nazwami: Trusted Computing, Trustworthy Computing, Palladium, NGSCB, Safer Computing

Ogólna idea

- Sprzętowe kodowanie danych z kluczem trzymanym poza dostępem użytkownika
- Sygnatura sprzętu sprawdzająca, czy nie ma nieuprawnionych komponentów
- Programy sprawdzające poprzez TC uprawnienia dostępu do danych oraz do możliwości ich wymiany
- Nowe reguły regularnie ściągane ze specjalnych serwerów – blokowanie tej akcji od razu obcina uprawnienia w systemie

Historia idei

- 1972 – James Anderson dla USAF
- 1997 – *The TrustNo 1 Cryptoprocessor Concept* Markusa Kuhna
- 1997 - Bill Arbaugh, Dave Farber i Jonathan Smith „A secure and reliable bootstrap architecture”

Czyli co to ma robić?

- Środowisko zabezpieczone przed użytkownikiem
- Pierwotny cel: DRM
- Odcięcie pirackiego oprogramowania, zabezpieczenie rejestracji programów, blokowanie plików tworzonych nielegalnym oprogramowaniem
- Zdalna cenzura – traitor tracing
- Zmiana podejścia do informacji: twórca jest jedynym zarządcą przez cały okres istnienia danych.

Możliwości TC

- Możliwość zagwarantowania, na jakich programach i na których komputerach można odczytać dane, przez jaki czas lub ile razy
- Separacja programów pomiędzy sobą nazwajem, gwarancja integralności danych
- Usprawnienie zbierania opłat za odtwarzanie muzyki i filmów, blokowanie przed wymianą takimi danymi
- Automatyczne niszczenie danych, zdalna kontrola nad odczytem danych (np. E-maile)

Czego nie daje TC?

- Wbrew wczesnym zapewnieniom MS nie broni przed wirusami
- Nie będzie chronić przed spamem

5 składników systemu TC

- hardware'owy układ Fritz z zaszytym kluczem i pewnymi danymi umożliwiającymi identyfikację
- Opcja „Curtained memory” zaszyta w procesorze
- Bezpieczne jądro systemu operacyjnego (w nazewnictwie MS „Nexus”)
- Bezpieczne jądro aplikacji (wg. nazewnictwa MS „NCA”)
- Struktura serwerów dostarczających reguły dla programów

Chip Fritz

- Kontrolowanie stanu komputera w trakcie startu systemu
- Udostępnienie kluczy deszyfrujących do systemu
- Sprawdzanie integralności danych oraz programów

Nexus

- Pośredniczy pomiędzy aplikacjami a Fritzem
- Bada zainstalowany sprzęt, czy jest dozwolony (duże zmiany sprzętu powodują konieczność ponownego uwerzytelnienia komputera w serwerach)
- Sprawdza, czy aplikacje są zarejestrowane i czy klucze nie są na czarnej liście
- Nadzoruje dostęp do pamięci dzięki „curtained memory”

Co się dzieje potem

- W zatwierdzonym stanie Fritz sprawdza uprawnienia i albo daje dostęp do danych albo jeszcze sprawdza uprawnienia z zewnętrznym serwerem
- Serwer na podstawie swojej polityki przyznaje uprawnienia
- Dane dostępne tylko dla zaufanych aplikacji i tylko tak długo, jak długo system jest w „zaufanym” stanie

Możliwości nadużyć

- Cenzura dokumentów
- Strategiczne blokowanie działania komputerów
- Blokowanie dokumentów wstecz
- Zmuszenie do używania konkretnego oprogramowania – wiązanie użytkowników do oprogramowania
- Całkowita kontrola przepływu informacji

Dlaczego tego używać?

Tak naprawdę z punktu widzenia użytkownika nie ma powodów za... Ale:

- Poprzez wiązanie użytkowników wymuszenie używania oprogramowania TC
- Organizacje typu RIAA, sklepy internetowe czy banki wyrażają zainteresowanie i mogą wymuszać korzystanie z TC
- Dla przedsiębiorstw możliwe za duże koszty rezygnacji – możliwa też utrata klientów

Science - Fiction?

Niestety nie:

- Numer seryjny Pentium 3 – pierwsze kroki
- 2000 – pierwsza gotowa specyfikacja
- Atmel już sprzedaje chipy Fritz, są one też już instalowane np. w laptopach IBM Thinkpad
- Konieczność reaktywacji przy zmianie sprzętu w Windows XP

Science – Fiction cd.

- Próby rejestracji wszystkich sterowników dla Windows – na razie tylko ostrzeżenie przy niezarejestrowanym sterowniku
- Obecne przy security patchu do Windows Media Player zapisy umożliwiają kontrolę zachowania WMP zdalnie
- Windows Server 2003 – obecna implementacja Enterprise Rights Management
- Longhorn ma mieć już w pełni zaimplementowane bezpieczne jądro

Więcej o TC

- www.trustedcomputinggroup.org – strona domowa TCG
- <http://www.gnu.org/philosophy/can-you-trust.html> - artykuł Richarda Stallmana nt. Treacherous Computing
- <http://www.cl.cam.ac.uk/%7Erja14/tcpa-faq.html> - FAQ nt. TC (od strony GNU, czyli znowu treacherous computing)