Kryptos - dane pod ochroną

Grzegorz "Krashan" Kraszewski

Jedną z nowych cech systemu MorphOS w wersji 2.2 jest Kryptos - system szyfrowania danych. Kryptos jest portem popularnego programu TrueCrypt, wydanego na systemy Windows, Linux i MacOS X. Kryptos zachowuje kompatybilność formatu partycji, a więc umożliwia dwustronną wymianę danych zaszyfrowanych na dyskach twardych, pamięciach USB, czy płytach CD i DVD między wszystkimi wymienionymi systemami. Dane można również wymieniać siecią, np. jako załączniki poczty albo poprzez serwisy hostujące pliki.

Jak to drzewiej bywało

Szyfrowanie danych to problem stary jak świat. Żartobliwie można by zacząć, że "już starożytni Rzymianie..." i byłaby to... prawda. Jeden z pierwszych znanych szyfrów to tak zwany szyfr Cezara, używany między innymi przez Juliusza Cezara, cesarza Rzymu. Jest on prymitywny z punktu widzenia współczesnej kryptografii, ale pokazuje, że potrzeba utajniania danych towarzyszy ludziom od dawna. Do końca XIX wieku szyfry były dość proste, bo szyfrowanie i rozszyfrowywanie wykonywano ręcznie. Dla potrzeb kryptografii szybko jednak wprzęgnięto osiągnięcia mechaniki precyzyjnej i elektrotechniki. W latach poprzedzających drugą wojnę światową zbudowano urządzenia elektromechaniczne do szyfrowania tekstu. Najsłynniejszym z nich była niemiecka "Enigma", której szyfr złamali polscy matematycy. Już w 1932 roku zespół kierowany przez Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego był w stanie odczytywać zakodowane depesze armii niemieckiej. Później na bazie ich wiedzy Anglicy zbudowali w czasie drugiej wojny światowej automatyczne urządzenia dekodujące. Warto zauważyć, że postęp techniczny z jednej strony pozwalał na używanie coraz bardziej złożonych szyfrów, ale z drugiej dawał do ręki kryptoanalitykom coraz skuteczniejsze narzędzia do ich łamania. Skonstruowanie komputerów przeniosło szyfry i kryptografię na kolejny poziom złożoności. Szybkość działania komputerów pozwalała na zastosowanie do łamania szyfrów metody "brute force" (na siłę, przez sprawdzenie wszystkich możliwych kombinacji). Z drugiej strony zbudowano szyfry, w których ilość tych możliwych kombinacji jest nieprawdopodobnie duża i wymaga setek tysięcy lat pracy współczesnych komputerów. Jak w wielu innych dziedzinach, w kryptografii trwa odwieczny wyścig zbrojeń, niczym walka między pancerzem a pociskiem w technice wojskowej.

Początkowo głównym zastosowaniem szyfrów było uniemożliwienie odczytania "nieprzyjacielowi" wiadomości przesyłanych jawnym kanałem (np. nadawanych przez radio). Tak było również po pojawieniu się komputerów, przede wszystkim szyfrowano wiadomości. Już w 1991 roku pojawiła się pierwsza wersja programu PGP (Pretty Good Privacy), przeznaczonego do szyfrowania poczty elektronicznej. Oczywiście to jeden z wielu podobnych programów, ale najbardziej znany ze względu na niezwykle skuteczne algorytmy i jedno z pierwszych popularnych zastosowań szyfrowania z parą kluczy - tajnym i jawnym. Rozgłosu dodał PGP fakt wdrożenia śledztwa przeciw autorowi, Phillowi Zimmermannowi, przez rząd USA. Zarzutem był nielegalny eksport technologii wojskowych. Śledztwo w końcu umorzono, a w międzyczasie Zimmermann zabezpieczył się w zabawny sposób - wydając książkę zawierającą... kompletny kod źródłowy PGP. Eksport książek jest jak najbardziej w zgodzie z amerykańskim prawem.

W miarę rozwoju komputerów, zwłaszcza osobistych, rozwijały się również pamięci masowe, gromadząc coraz więcej danych. Komputery stawały się coraz mniejsze, pojawiły się laptopy. Dane znajdujące się na ich dyskach są nieraz warte miliony dolarów. O ile trudno sobie wyobrazić kradzież dysku twardego o pojemności 5 MB i wadze 50 kg z centrum komputerowego (napędy z lat siedemdziesiątych XX wieku), o tyle kradzież laptopa nie jest problematyczna. Pal licho samego laptopa, ale kradzież danych np. biznesowych, może przynieść ogromne straty. Obejście hasła, powiedzmy, systemu Windows, to żadna filozofia. Zabezpieczyć przed skutkami kradzieży może tylko szyfrowanie danych na dysku.

Idea działania

Kryptos - dane pod ochroną

Grzegorz "Krashan" Kraszewski

Początkowo szyfrowaniu poddawano pojedyncze pliki. Najczęściej operacja szyfrowania jest połączona z kompresją danych. Zgodnie z teorią kryptografii, bezstratna kompresja danych przed szyfrowaniem zwiększa "siłę" szyfru, utrudniając atak. Dzieje się tak dlatego, że kompresja usuwa powtarzające się dane i ujednolica statystyczny rozkład symboli w szyfrowanej wiadomości. Dlatego niemal każdy program szyfrujący jest jednocześnie kompresorem. Szyfrowanie pojedynczych plików umożliwiał na Amidze już słynny PowerPacker, również do XPK mamy moduły szyfrujące. Opcję zaszyfrowania hasłem znajdziemy również w kompresorach popularnych na innych platformach (ZIP, RAR). Niemniej siła szyfrowania używanego w tych programach nie jest zbyt wielka, o czym świadczy spora liczba skutecznych programów do łamania haseł. Również wygoda pracy nie jest wstrząsająca. Jeżeli np. pracujemy nad tajnym dokumentem tekstowym, przed każdym rozpoczęciem pracy musimy rozszyfrować plik, a następnie zaszyfrować go na zakończenie. Dodatkowo ryzykujemy zapomnieniem o skasowaniu rozszyfrowanej wersji oraz tym, że zdolny człowiek znajdzie na dysku tę rozszyfrowaną wersję nawet po jej skasowaniu.

Współczesne oprogramowanie szyfrujące działa w inny, znacznie wygodniejszy sposób. Szyfrowanie odbywa się na poziomie partycji dysku. Program szyfrujący tworzy w systemie wirtualną partycję. Aplikacje traktują ją tak, jak zwykły wolumen, ale wszystkie dane zapisywane na taką partycję są automatycznie szyfrowane. Przy odczycie rozszyfrowywanie odbywa się również "w locie". Co ważne, dane jawne nigdy nie trafiają na dysk, istnieją tylko w pamięci RAM komputera, a więc znikają po jego wyłączeniu (jest to pewne uproszczenie, o czym niżej). Jak wiadomo, dane zapisane na dysku twardym są często możliwe do odtworzenia, nawet po fizycznym nadpisaniu zawierających je sektorów dysku. Programy takie jak TrueCrypt gwarantują, że dane w postaci jawnej nigdy nie zostaną zapisane w pamięci masowej. Szyfrowane są nie tylko same pliki, ale również cała struktura systemu plików i drzewo katalogów wraz z ich nazwami.

TrueCrypt

Każdy z bardziej znaczących współczesnych systemów operacyjnych oferuje jakieś oprogramowanie szyfrujące, opierające się na zasadzie szyfrowania partycji "w locie". W Windows Vista jest to BitLocker, MacOS X posiada FileVault, a Linux dm-crypt. Programy te są wzajemnie niekompatybilne między sobą, poza tym BitLocker i FileVault mają zamknięty kod źródłowy, mogą więc zawierać tak zwane "tylne wejścia" (ang. "backdoors"), umożliwiające rozszyfrowanie danych twórcom, czy wydawcom systemu operacyjnego albo agencjom rządowym. Z tych zapewne powodów pojawił się TrueCrypt. Jest to oprogramowanie darmowe, o otwartych kodach źródłowych. Doczekało się portów zarówno na Windows, Linuksa, jak i MacOS X. Co więcej, zachowano kompatybilność formatu danych, więc dane zaszyfrowane pod jednym z tych systemów, odczytamy pod każdym z pozostałych. Wraz z Kryptosem dołącza do nich MorphOS, kompatybilność mamy w obie strony.

Jak wcześniej wspomniałem, TrueCrypt tworzy w systemie dodatkowe wirtualne partycje dysków. Partycje te mogą być przechowywane na dysku na dwa sposoby. Mamy tu pewną analogię do emulatora UAE. Wirtualna partycja może odpowiadać rzeczywistej partycji dysku, może być również plikopartycją, a więc istnieć jako zwykły plik na niezaszyfrowanej partycji. Ten drugi sposób jest szczególnie wygodny w przypadku przenoszenia danych między komputerami. Plikopartycję możemy skopiować spod MorphOS-a na dowolny nośnik, powiedzmy pendrive, po czym zamontować ją TrueCryptem np. na Windows. Trzeba jednak pamiętać o ograniczeniu rozmiaru pliku - pod wieloma systemami plików możemy mieć problem z plikiem większym niż 2 GB. Jeżeli zaszyfrujemy całą, kompletną partycję, jej limit wielkości jest znacznie większy (np. partycja w systemie SFS może mieć do 128 GB). TrueCrypt w wersji dla Windows pozwala również na zaszyfrowanie partycji systemowej, dzięki czemu zaszyfrowany jest również plik wymiany (pamięć wirtualna na dysku). Kryptos nie posiada niestety takiej opcji. Z drugiej strony odpada problem z plikiem wymiany, w MorphOS-ie znacznie łatwiej też uniknąć zapisywania ważnych danych na partycji systemowej, bo mamy zdecydowanie większą kontrolę nad tym, gdzie są zapisywane np. pliki tymczasowe.

Kryptos - dane pod ochroną

Grzegorz "Krashan" Kraszewski

Dostęp do zaszyfrowanych danych w TrueCrypt może być chroniony hasłem, plikiem-kluczem, bądź hasłem i kluczem (lub kilkoma kluczami) jednocześnie. Kluczem może być dowolny plik na niezaszyfrowanym nośniku. Plik taki powinien mieć co najmniej 30 bajtów. Początek pliku powinien zawierać w miarę przypadkowe dane (najlepiej posłużyć się plikiem z kompresją danych, np. obrazkiem JPEG czy PNG, plikiem muzycznym MP3, jakimś archiwum). TrueCrypt nie zmienia zawartości klucza, zatem dla niepoznaki można użyć np. ikonki PNG albo jakiegoś pliku systemowego. Trzeba jednak uważać, aby zawartość pliku nie uległa przypadkowej zmianie. Jeżeli np. ktoś wybierze jedną z systemowych bibliotek jako klucz, a następnie zaktualizuje MorphOS-a, co spowoduje nadpisanie biblioteki nową wersją, zaszyfrowane dane staną się niedostępne. Również zapisanie tooltypu (albo czegokolwiek innego, np. zmiana typu ikony lub domyślnego narzędzia) do ikony zepsuje nasz klucz i zablokuje dostęp do danych. Przy wyborze pliku na klucz trzeba więc chwilę pomyśleć, aby uniknąć kłopotów.

Kryptos

TrueCrypt został przeportowany na MorphOS-a przez Marka Szyprowskiego i ochrzczony nazwą Kryptos. Nie był to tak zwany szybki port - Kryptos jest w pełni przystosowany do współpracy i zintegrowany z MorphOS-em. Interfejs graficzny programu zbliżony jest do wersji na inne systemy, ale korzysta oczywiście z MUI. Montowane partycje są widziane jako najzwyklejsze urządzenia DOS-a, a ich nazwy możemy sobie sami ustalić. W systemie możemy mieć maksymalnie 16 zaszyfrowanych partycji.

Rys. 1

Pracę zaczynamy od wyboru między plikopartycją a zaszyfrowaniem partycji rzeczywistej. Zaletą plikopartycji jest przenośność, pełna kontrola nad rozmiarem i - co ważne dla początkujących - niewielkie ryzyko zepsucia czegoś na dysku. Wadą jest przede wszystkim ograniczony rozmiar. Różnica w szybkości dostępu do danych jest niewielka. W przypadku tworzenia plikopartycji, wskazujemy miejsce na dysku, gdzie chcemy ją stworzyć (rys. 7), jeżeli szyfrujemy partycję rzeczywistą, partycję dysku wybieramy poprzez urządzenie logiczne RAWDISK: (rys. 2.). Dla plikopartycji możemy następnie ustalić rozmiar (rys. 10.) (wolumen TrueCrypta założony na rzeczywistej partycji zawsze zajmuje całą partycję, jak widać na rys. 3.).

Rys. 2

Następnym krokiem jest wybór szyfru i funkcji skrótu (rys. 4.). W sieci można znaleźć szereg rozważań i porównań dostępnych szyfrów (są to AES, Serpent i Twofish oraz wzajemne kombinacje dwóch i trzech z nich). W praktyce wystarczy dowolny, osoby kładące szczególny nacisk na bezpieczeństwo danych mogą użyć kombinacji, pamiętając, że zwiększa to nieco obciążenie procesora, co może być ważne przy wolnych komputerach (np. Efika). Bardzo istotny jest natomiast wybór rodzaju formatowania. W przypadku plikopartycji jesteśmy tego wyboru pozbawieni. Szyfrując rzeczywistą partycję powinniśmy zawsze wybrać formatowanie standardowe. Cała partycja przed stworzeniem systemu plików zostaje wtedy wypełniona losowymi danymi. Trwa to, co prawda od kilku minut do nawet kilku godzin, ale jest niezbędne do zapewnienia bezpieczeństwa danych. Jeżeli pójdziemy na łatwiznę i wybierzemy szybkie formatowanie, atak na nasze dane będzie bardzo ułatwiony. Wyjątek możemy zrobić tylko jeśli partycja już zawiera losowe dane (np. była już wcześniej formatowana TrueCryptem albo jakąś inną aplikacją zapisującą dane losowe).

Rys. 3

Dochodzimy teraz do ustalenia hasła i klucza (rys. 5.). Klucz jest niewątpliwie wygodniejszy, jednak musimy mieć pewność, że plik klucza nie zostanie przypadkowo zmieniony, o czym wspomniałem wyżej. Poza tym klucz może być łatwiejszy do przechwycenia, jeżeli ktoś zorientuje się, jaki plik nim jest. Wtedy wystarczy kradzież komputera, jeżeli

używamy hasła, pozostaje ono (a przynajmniej pozostawać powinno) wyłącznie w naszej pamięci. Można też użyć i klucza i hasła, a nawet kilku kluczy (rys. 6.). W ten sposób można np. tworzyć partycje, do których dostęp ma kilka osób - ale tylko wtedy, gdy wszyscy wyrażą zgodę, udostępniając swoje klucze. Tworząc hasło - unikajmy prostych wyrazów i oczywistych kombinacji z datą urodzin itp. Dość skutecznym, a przy tym w miarę łatwym do zapamiętania hasłem jest dłuższe zdanie lub tytuł, zwłaszcza jeżeli przekręcimy kilka liter albo wstawimy kilka cyfr. Hasło powinno być zdecydowanie dłuższe niż 8 znaków. Jeżeli zaszyfrowane dane będziemy przenosić między różnymi systemami operacyjnymi, nie używajmy w haśle polskich znaków, gdyż może to spowodować problemy.

Rys. 4

Kolejną czynnością jest określenie parametrów systemu plików (rys. 11.). Jeżeli dane będziemy wymieniać z innymi systemami, niemal oczywistym wyborem jest FAT32, podobnie jak to robimy w przypadku nośników USB. Dla partycji na nośnikach nieprzenośnych, montowanych tylko pod MorphOS-em, wybrać można SFS. Wybór systemu plików nie ma wpływu na łatwość złamania szyfru. Nazwa urządzenia oraz etykieta partycji nie wymagają chyba komentarza.

Rys. 5

Na bazie hasła i kluczy Kryptos generuje klucz główny wolumenu, który w postaci zaszyfrowanej umieszczony jest razem z danymi. Aby utrudnić złamanie klucza głównego, generator liczb losowych wspomagany jest losowością pochodzącą od człowieka. Kryptos prosi użytkownika o wykonanie kilkunastu chaotycznych ruchów myszą. Oczywiście nie trzeba wymachiwać na całą szerokość biurka, wystarczą spokojne, ale niespecjalnie mierzone ruchy w różnych kierunkach. Po wygenerowaniu klucza, Kryptos przystępuje do formatowania partycji (rys. 7). Tu trzeba się uzbroić w cierpliwość - formatowanie np. 20 GB na Efice może potrwać kilka godzin.

W działaniu

Po przygotowaniu partycji możemy ją zamontować w systemie, korzystając z głównego okna Kryptosa (rys. 1.). Po dwukliku w partycję na liście, zostaniemy poproszeni o hasło (albo nie, jeżeli partycja jest zabezpieczona tylko kluczem w pliku). Po podaniu prawidłowego hasła na blacie Ambienta pojawi się ikona naszej partycji. I to wszystko - dalej używamy jej jak każdej innej.

Rys. 6

Czy musimy odmontować partycję przed wyłączeniem komputera? W zasadzie nie, chociaż wykonanie tej czynności znacznie utrudnia część ataków na dane, o czym niżej. Dodatkowo podobnie jak w przypadku zwykłych partycji, wyłączenie komputera w czasie trwającego zapisu może nam uszkodzić system plików z wszystkimi tego smutnymi konsekwencjami. Dlatego najbezpieczniej jest odmontować albo wyjść z Kryptosa poprzez opcję w menu, co automatycznie odmontuje wszystkie zaszyfrowane wolumeny.

Rys. 7

Jest rzeczą jasną, że szyfrowanie danych musi wprowadzać pewne opóźnienia. Aby pokazać szybkość Kryptosa, przygotowałem tabelkę przedstawiającą wyniki pomiarów na Pegasosie 2 i Efice. Dla porównania podałem również szybkość kopiowania plików bez szyfrowania oraz szybkość odczytu z dysku mierzoną programem SCSISpeed. To pozwala w pewnym stopniu uwzględnić wpływ szybkości samego dysku.

Kopiowany był zestaw 12 plików muzycznych o łącznej wielkości 158,3 MB. Pegasos 2 posiada dysk Seagate

Kryptos - dane pod ochroną

Grzegorz "Krashan" Kraszewski

Barracuda o pojemności 60 GB (7200 rpm, 8 MB cache), Efika posiada dysk Samsung (2,5 cala) o pojemności 40 GB (5400 rpm, również 8 MB cache). Wszystkie szyfrowane partycje użyte w tym teście były partycjami rzeczywistymi. Użyłem pojedynczego szyfru AES i funkcji skrótu SHA-512. Testy powtórzyłem kilkakrotnie, w tabelce znajdują się wartości średnie.

Pegasos 2 Efika SCSISpeed (bufor 32 kB) 40,0 MB/s 5,2 MB/s kopiowanie danych z partycji zwykłej na zwykłą 16,2 MB/s 2,6 MB/s kopiowanie danych z partycji zwykłej na szyfrowaną 7,5 MB/s 1,3 MB/s kopiowanie danych z partycji szyfrowanej na zwykłą 6,8 MB/s 1,3 MB/s kopiowanie danych z partycji szyfrowanej na szyfrowaną 4,8 MB/s 1,0 MB/s

Jak widać, spowolnienie kopiowania danych wnoszone przez Kryptosa jest spore i należy je wziąć pod uwagę. W przypadku obu komputerów szyfrowanie po jednej stronie (odczyt lub zapis) powoduje zmniejszenie transferu mniej więcej o 50 do 60%. Dodatkowo w przypadku Pegasosa zwykłe kopiowanie danych w niewielkim stopniu angażuje procesor, kopiowanie danych z partycji szyfrowanej na szyfrowaną oznacza obciążenie procesora około 80%.

Rys. 8

Ataki na TrueCrypta

Czy TrueCrypt, a tym samym Kryptos, jest bezpieczny? Czy możliwy jest udany atak i przejęcie danych? Zwróćmy uwagę na istotny fakt - TrueCrypt chroni dane na dysku, ale nie chroni danych w pamięci RAM komputera. W pamięci tej znajdują się nie tylko tymczasowe bufory na ostatnio zapisywane i odczytywane dane. Znaleźć tam można również rozszyfrowany klucz główny. Oczywiście nic to nie zmienia w czasie, gdy zaszyfrowana partycja jest zamontowana w systemie. Wtedy każdy, kto ma fizyczną, lub zdalną kontrolę nad komputerem, jest w stanie czytać chronione dane. W praktyce haker może więc, zamiast próbować ataku na sam szyfr, umieścić w systemie trojana, który poczeka, aż użytkownik zamontuje zaszyfrowaną partycję. Wtedy trojan może po prostu skopiować dowolne dane i przesłać siecią do hakera. Trojan może też odnaleźć w pamięci aktywny klucz główny i przesłać go hakerowi. Klucz można później wykorzystać na przykład po kradzieży komputera. Jak widać, nie można bezkrytycznie traktować Kryptosa jako cudownego zabezpieczenia danych. Daje on pewność tylko w przypadku, gdy komputer w momencie przejęcia nad nim kontroli przez nieuprawnione osoby, jest wyłączony, bądź jest włączony, ale zaszyfrowane partycje nie są zamontowane w systemie.

Rys. 9

Ciekawym przykładem udanego ataku na TrueCrypta jest eksperyment przeprowadzony przez naukowców z Princeton University. Dotyczy on jednej z typowych sytuacji, gdy komputer jest włączony, a szyfrowane partycje są zamontowane. Nagle do drzwi puka (albo, co gorsza, te drzwi wyważa) ekipa z nakazem rewizji (albo i bez nakazu, różnie w życiu bywa, w zależności od czasu i miejsca...). Błyskawicznie wyrywamy wtyczkę z kontaktu, wyłączając w ten sposób wszystkie komputery z krytycznymi danymi i z uśmiechem witamy w drzwiach panów w czarnych płaszczach. Czy aby do końca z uśmiechem? Powszechna wiedza o dynamicznych pamięciach RAM używanych obecnie w komputerach mówi, że wymagają one odświeżania zawartości co kilkadziesiąt milisekund i tracą zawartość od razu po wyłączeniu zasilania. Nie jest to, jak się okazało, prawdą. Pamięć zachowuje zawartość nie tylko po wyłączeniu zasilania, ale nawet po wyjęciu jej z komputera i włożeniu do drugiego, co umożliwia wykonanie zrzutu zawartości pamięci "zamrożonej" w momencie zaniku zasilania. Jest to również możliwe w prostszy sposób, przez natychmiastowe wystartowanie komputera ze specjalnie spreparowanego minisystemu (np. przez USB), którego jedynym zadaniem jest zrzucenie zawartości pamięci. W prostej linii prowadzi to do zdobycia klucza TrueCrypta.

Kryptos - dane pod ochroną

Grzegorz "Krashan" Kraszewski

Rys. 10

Jak długo pamięć potrafi przetrzymać dane po odcięciu zasilania? W zależności od rodzaju pamięci (nowsze trzymają krócej) jest to od kilku do kilkudziesięciu sekund w temperaturze pokojowej. Pamięci DDR2 przechowują dane około 2 sekund po odcięciu zasilania. Prosty zabieg polegający na schłodzeniu pamięci tak zwanym "sprężonym powietrzem" w sprayu (trzymając puszkę do góry nogami, wtedy wylatuje z niej czynnik sprężający oprócz powietrza) przed wyłączeniem komputera pozwala na osiągnięcie temperatury około -50°C. W takiej temperaturze pamięci zachowują zawartość przez kilka minut. Jeżeli tak wstępnie schłodzony moduł pamięci wyjmiemy z komputera i bezzwłocznie umieścimy w ciekłym azocie (-196°C), zawartość pamięci jest utrzymywana bez zasilania przez kilka godzin z ilością błędnych bitów poniżej 0,01%.

Rys. 11

Eksperymentatorzy wykonywali kompletny zrzut pamięci komputera, używając opisanych wyżej sztuczek z chłodzeniem. Następnie, posługując się napisanym przez siebie oprogramowaniem, odszukiwali klucz główny zaszyfrowanej partycji. Istnieje oczywiście możliwość, że kilka bitów klucza zdążyło się już "uszkodzić", jest jednak na to sposób. Oprogramowanie szyfrujące takie jak TrueCrypt, oprócz głównego klucza, trzyma w pamięci szereg kluczy pomocniczych wyliczanych z głównego, a służących do przyspieszenia operacji szyfrowania i rozszyfrowywania danych. Naukowcy z Princeton z sukcesem wykorzystali te klucze do korekcji błędów w kluczu głównym. Swoje dokonania udokumentowali w publikacji naukowej, a także sfilmowali, a filmy umieścili na YouTube.

Materiały źródłowe:
J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, E. W. Felten, "Lest We Remember: Cold Boot Attacks on Encryption Keys", publikacja opisująca szczegółowo atak na systemy szyfrowania dysków metodą zrzutu pamięci.
Film pokazujący metody ataku na oprogramowanie szyfrujące poprzez pamięć RAM.
Strona poświęcona eksperymentowi ze schładzaniem modułów pamięci RAM.
Strona domowa programu TrueCrypt

Artykuł oryginalnie pojawił się w drugim numerze Polskiego Pisma Amigowego.