Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- Czym jest kryptografia?
- Szyfrowanie zapisanych danych
- Szyfrowanie informacji w podróży
- Dobre praktyki i zalecenia

Zrozumieć kryptografię

REDAKTOR GOŚCINNY

Redaktorem gościnnym tego numeru OUCH! jest Fred Kerby. Ostatnio zakończył on pracę w centrum Naval Surface Warfare Center, w wydziale Dahlgren, gdzie służył na stanowisku Information Assurance Manager przez 16 lat. Teraz jest starszym instruktorem w Instytucie SANS.

CZYM JEST KRYPTOGRAFIA?

Kryptografia to mechanizm pozwalający chronić cenne informacje – takie jak na przykład dokumenty, zdjęcia lub transakcje przeprowadzane online - przed osobami, które chcą uzyskać do nich dostęp lub zmienić ich treść bez naszej wiedzy i pozwolenia. Kryptografia polega na wykorzystaniu szyfru (matematycznego przekształcenia) w połączeniu z kluczem do przekształcenia danych z ich czytelnej postaci (tekstu jawnego) na postać niezrozumiałą dla innych (szyfrogram). Sam szyfr jest tylko ogólnym algorytmem kryptograficznym - recepturą. Klucz natomiast jest jego parametrem, elementem, który czyni zaszyfrowane dane określoną, niepowtarzalną treścią. Tylko osoby dysponujące określonym kluczem przy wykorzystaniu tego samego szyfru mogą tą treść odczytać. Kluczami są zazwyczaj ciągi liczb zabezpieczone przez mechanizmy uwierzytelniające oparte o hasła, tokeny albo dane biometryczne, jak na przykład mechanizmy przetwarzające informacje o odcisku palca.

SZYFROWANIE ZAPISANYCH DANYCH

Możliwe, że przechowujesz ważne informacje na urządzeniu przenośnym, takim jak na przykład laptop, pendrive, smartphone lub tablet. Urządzenia tego typu są często gubione lub mogą zostać skradzione. W takich sytuacjach każda osoba, która ma do nich dostęp, może próbować odczytać zapisane na nich informacje. Jedną z najlepszych metod zabezpieczania danych na urządzeniach przenośnych jest szyfrowanie.

Można wyróżnić trzy metody szyfrowania danych na urządzeniach przenośnych. Możesz zaszyfrować konkretne pliki, całe foldery lub cały twardy dysk. Większość systemów operacyjnych dostarcza jednej, jeśli nie wszystkich trzech metod. Szyfrowanie całego dysku (FDE – ang. Full Disk Encryption) jest często uważane za najbezpieczniejsze. FDE szyfruje wszystkie dane na Twoim dysku, włączając w to pliki tymczasowe. Sposób ten upraszcza także proces zabezpieczania, ponieważ nie musisz się zastanawiać, co szyfrować, a czego nie. Jeśli nie możesz zaszyfrować całego dysku, zaszyfruj pliki lub foldery, które zawierają wrażliwe informacje. Przenośne urządzenia, takie jak napędy USB, czasami posiadają wbudowane mechanizmy szyfrujące lub też można zainstalować na nich odpowiednie aplikacje (tzw. “appy”) -

Zrozumieć kryptografię

tych należy szukać w “app store'ach” lub “marketplace'ach” danego producenta.

SZYFROWANIE INFORMACJI W PODRÓŻY

Informacja jest też bardziej podatna na ataki kiedy jest udostępniana osobom będącym w podróży. Jeśli nie jest ona szyfrowana, może być obserwowana i zostać przechwycona. Właśnie dlatego wszystkie Twoje ważne połączenia, takie jak: bankowość online, wysyłane maile, być może nawet dostęp do Twojego konta na Facebook, powinny być szyfrowane. Najpopularniejszym sposobem szyfrowania połączeń jest używanie protokołu HTTPS. Dzięki temu połączenie pomiędzy Twoją przeglądarką a serwerem jest szyfrowane. Aby upewnić się, że używasz HTTPS, w adresach URL w przeglądarce szukaj łańcucha https:// lub ikony kłódki. Wiele witryn zapewnia tą metodę domyślnie (np. Google Apps), a strony takie jak Facebook czy Twitter oferują możliwość włączenia opcji wymuszania połączeń HTTPS. Dodatkowo, jeśli podłączasz się do publicznych sieci Wi-Fi, używaj szyfrowania kiedy tylko jest to możliwe. WPA2 jest w tej chwili jednym z najsilniejszych mechanizmów szyfrujących w sieciach radiowych i właśnie jego powinieneś używać. Wreszcie, kiedy wysyłasz i odbierasz maile, upewnij się, że Twój klient pocztowy jest skonfigurowany tak, by używał szyfrowanych kanałów transmisji. Jednym z najczęściej wybieranych protokołów zabezpieczających połączenia z serwerami pocztowymi jest SSL (Secure Socket Layer). Wiele klientów pocztowych używa SSLa domyślnie.

DOBRE PRAKTYKI I ZALECENIA

Niezależnie od tego, jakiej formy szyfrowania używasz, jest kilka rzeczy, o których powinieneś pamiętać.

- Twój szyfr jest tylko tak silny, jak Twój klucz. Jeśli klucz zostanie skompromitowany, to samo stanie się z Twoimi danymi. Jeśli używasz haseł do ochrony Twoich kluczy, upewnij się, że są to silne hasła i że są dobrze chronione (zobacz: OUCH! numer majowy 2011 poświęcony hasłom).

Szyfrowanie to doskonałe narzędzie ochrony danych. Jednak jego efektywność zależy od siły naszych kluczy i stanu zabezpieczeń całego systemu operacyjnego.

- Uważaj, by nie stracić kluczy lub dostępu do nich. Jeśli stracisz klucze szyfrujące lub stracisz do nich dostęp z powodu zapomnianego hasła, prawdopodobnie nie będziesz w stanie odzyskać zabezpieczonych danych.

- Twój szyfr jest tylko tak silny jak zabezpieczenia Twojego komputera. Jeśli Twój komputer jest zainfekowany, intruzi mogą skompromitować Twój szyfr.

- Pamiętaj, by utrzymywać ogólną ochronę Twojego systemu. Kryptografia nie chroni przed wirusami, robakami, trojanami, niezałatanymi lukami ani przed inżynierią społeczną.

Zrozumieć kryptografię

- Pamiętaj, by robić backup swoich danych. Dzięki temu, nawet jeśli stracisz klucze lub swoje urządzenie przenośne, nadal będziesz mógł odzyskać dane.

- Używaj raczej szyfrów opartych o otwarte standardy, jak AES (ang. Advanced Encryption Standard) lub Blowfish niż tych korzystających z protokołów własnościowych. Upewnij się też, czy masz najnowszą wersję oprogramowania szyfrującego.

- Jeśli zajdzie taka potrzeba, poproś o pomoc profesjonalnego informatyka. Niepoprawna instalacja oprogramowania, konfiguracja lub niepoprawne używanie może doprowadzić do utraty danych.

ZASOBY

Niektóre z podanych poniżej linków zostały skrócone dla zwiększenia czytelności przy użyciu usługi TinyURL. Ze względów bezpieczeństwa OUCH! zawsze korzysta z usługi podglądu TinyURL, która pokazuje ostateczną lokalizację wskazywaną przez link i pyta się o pozwolenie zanim ją otworzy.

Narzędzia FDE (pełne szyfrowanie dysku):
TrueCrypt: http://www.truecrypt.org/
PGP: http://www.pgp.com
Windows 7 Bitlocker: http://preview.tinyurl.com/3xaubbr

Szyfrowanie plików i folderów:
TrueCrypt: http://www.truecrypt.org/
Windows: http://preview.tinyurl.com/yb29rzn
Mac: http://preview.tinyurl.com/6c2q3cy

Szyfrowanie nośników USB:
TrueCrypt: http://www.truecrypt.org/
SanDisk: http://preview.tinyurl.com/3nl4g2p
IronKey: https://www.ironkey.com/products

Standardy kryptograficzne:
AES: http://preview.tinyurl.com/ku33x
WiFi: WPA oraz WPA2 http://preview.tinyurl.com/am5oa
Jak działa HTTPS: http://preview.tinyurl.com/ya9se7f
Jak działa VPN: http://preview.tinyurl.com/rfc9f

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

POLSKI PRZEKŁAD

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagownia na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet.
Należy do organizacji FIRST w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Polski przekład (NASK/CERT Polska): Tomasz Sałaciński