CC BY ND

ISSN 2080-1807

TORUŃSKIE STUDIA BIBLIOLOGICZNE
2017, nr 1 (18)

Mariusz Jarocki
Instytut Informacji Naukowej i Bibliologii
Uniwersytet Mikołaja Kopernika w Toruniu
e-mail: maryan@umk.pl

Czy technologiczne aspekty działania programów informacyjno-komunikacyjnych powinny być znane tylko wybrańcom?

DOI: http://dx.doi.org/10.12775/TSB.2017.011

Streszczenie: Nie każdy potrafi napisać program komputerowy, to wydaje się kwestią oczywistą. Jednak czy większość osób nie posiadających wykształcenia technicznego (lub ścisłego) nie powinna poznać podstawowych zasad, według których on działa? Otóż, dlaczego nie? Z tym wydaje się trudnym z założenia zadaniem postanowił zmierzyć się autor publikacji *Jak działa oprogramowanie? Tajemnice komputerowych mechanizmów szyfrowania, obrazowania, wyszukiwania i innych powszechnie używanych technologii.* Opierając się na prostych, znanych z życia codziennego przykładach, postanowił przybliżyć te mechanizmy działania programów komputerowych, które jego zdaniem są najpopularniejsze i mogą zaciekawić czytelnika.

Słowa kluczowe: cyberbezpieczeństwo, multimedia, technologie komunikacyjno-informacyjne.

Oprogramowanie jest nieodłączną częścią składową systemu komputerowego, bez niego nie ma możliwości użytecznego wykorzystania komputera. Najważniejszą częścią programu są natomiast składające się na niego algorytmy, które stanowią swoisty przepis na wykonanie czynności, do których została przeznaczona aplikacja. Algorytm jest rozwiązaniem problemu, najczęściej ujętym w sposób łatwy do zapisania

matematycznie. W publikacji V. Antona Spraula[1] podjęta została próba opisania działania takich matematycznych przepisów w oparciu o sytuacje zaczerpnięte z życia codziennego. Według autora istotnym, o ile nie najważniejszym czynnikiem w działaniu wyżej wspomnianych systemów komputerowych, jest obsługujący je świadomy użytkownik. Głównym celem książki *Jak działa oprogramowanie? Tajemnice komputerowych mechanizmów szyfrowania, obrazowania, wyszukiwania i innych powszechnie używanych technologii* stała się właśnie edukacja człowieka obsługującego aplikacje – obecnie każdego z nas. V. A. Spraul wybrał kilka zagadnień, które uznał za najbardziej znaczące we współczesnej informatyce i związane z przetwarzaniem informacji. Zauważył równocześnie, że opisanie na łamach jednej publikacji wszystkich aspektów działania oprogramowania istotnych dla wielu potrzeb i sfer aktywności człowieka jest niemożliwe. Nie sposób się z tym stwierdzeniem nie zgodzić. Kwestią sporną dla czytelnika może się okazać tylko dobór omawianych typów oprogramowania. W książce podjęto próbę przybliżenia takich zagadnień, jak: szyfrowanie, hasła, bezpieczeństwo w sieci, film generowany komputerowo, grafika gier, kompresja danych, wyszukiwanie, współbieżność oraz trasy na mapach.

Pierwszy blok tematyczny składa się z trzech rozdziałów dotyczących szeroko pojętych sposobów na zapewnienie bezpieczeństwa informacji. Rozdział *Szyfrowanie* stanowi wprowadzenie w ogólne mechanizmy stosowane obecnie w celu zachowania poufności informacji. Autor rozpoczął prezentację zastosowania kryptografii od przykładów poprzedzających czasy komputerowe, następnie przeszedł do rozwiązań stosowanych obecnie. Pokazał, na czym polega proces szyfrowania i deszyfrowania, oraz – co najistotniejsze – wskazał czytelnikowi mocne i słabe strony przetestowanych metod. Kwestie matematyczne, których znajomość jest tu nieodzowna, wprowadził w sposób umiejętny i nie przytłaczający nawet dla osób nie posiadających wykształcenia ścisłego. Dokładnej analizie autor poddał sposób działania powszechnie stosowanego szyfrowania AES[2].

---

[1] V. A. Spraul, *Jak działa oprogramowanie? Tajemnice komputerowych mechanizmów szyfrowania, obrazowania, wyszukiwania i innych powszechnie używanych technologii*, Gliwice 2016.

[2] Por. *Announcing the ADVANCED ENCRYPTIN STANDARD (AES)* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Drugi rozdział *Hasła* wskazuje na niebezpieczeństwa związane z nieautoryzowanym dostępem do informacji. Niewątpliwie każdy użytkownik współczesnych systemów komputerowych słyszał o wycieku danych z kont użytkowników, a tym samym kwestiach wskazujących, że obecnie stosowane rozwiązania nie należą do zapewniających pełną niezawodność. Autor opisuje zasady tworzenia dobrze zabezpieczonych haseł przy użyciu metod haszowania (w szczególności md5[3]) oraz wyjaśnia, na czym polega działanie podpisów cyfrowych. Oprócz prezentacji metod zabezpieczających uwierzytelnianie do systemów komputerowych omówiono także sposoby, w jakie mogą one zostać przełamane, m.in. poprzez zastosowanie metody słownikowej czy atakom poprzez wywołanie kolizji.

Tematem trzeciego rozdziału tej części publikacji jest bezpieczeństwo w sieci. Przybliżone zostały tutaj działania kryptograficzne oparte na kluczu publicznym i prywatnym, podstawy bezpiecznej wymiany informacji oraz jak systemy rozpoznają, że nikt nie podszywa się pod właściciela lub odbiorcę wiadomości. Kwestie te autor szczegółowo omawia na przykładzie najpopularniejszej metody w tym zakresie – RSA[4]. V. Anton Spraul nie mniej uwagi poświęcił na protokoły zabezpieczonej wymiany informacji odbywającej się za pośrednictwem usługi WWW – protokołowi HTTPS[5].

Drugi blok zagadnień, poświęcony oprogramowaniu pozwalającemu na sprawne przetwarzanie danych multimedialnych, rozpoczyna rozdział *Film CGI*. Poświęcony jest on tematyce generowania obrazów metodą komputerową oraz powstających na ich podstawie animacji. Autor przybliża zakres pojęć, takich jak *bitmapa*, *klatka kluczowa*, *rozdzielczość*, *addytywne mieszanie kolorów*, *twining czy interpolacja*. Coraz większą część zasobów sieci stanowią zasoby graficzne i wideo. Stąd też przybliżenie tego zagadnienia na łamach niniejszej książki wydaje się zasadne. Niemniej jednak w tym przypadku rozczarowuje uboga szata graficzna publikacji. Podczas omawiania zmian kolorystycznych czy prezentacji

---

[3] Por. J. Black, M. Cochran, T. Highland, *A Study of the MD5 Attacks: Insights and Improvements* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://www.cs.colorado.edu/~jrblack/papers/md5e-full.pdf.

[4] Por. *PKCS #1 v2.1: RSA Cryptography Standard* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf.

[5] Por. *HTTP Over TLS* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: https://tools.ietf.org/ html/rfc2818.

najbardziej zachwycających kadrów filmów byłoby wskazane, by opublikowano je w kolorze i na papierze pozwalającym uzyskać lepszą jakość druku. Z całą pewnością można dokonać prawidłowej analizy efektów ostrości obrazu, jego odbicia czy zachowania przy różnych rodzajach oświetlenia na przykładach wydrukowanych w odcieniach szarości, ale nie powoduje to już tak dobrego efektu wizualnego.

Rozdział *Grafika gier* nie wydaje się początkowo związany z jakimkolwiek innym aspektem sfery życia człowieka niż rozrywkowy. Autor w tej części publikacji wykazuje, że generowanie grafiki filmowej wymaga bardzo wydajnego sprzętu komputerowego oraz dużo czasu. Natomiast w przypadku gier komputerowych obraz musi powstawać w czasie rzeczywistym, a tak dokładne odwzorowanie rzeczywistości jest obecnie nieosiągalne. Wyjaśnia, jakie zabiegi i metody są stosowane, by sprostać rosnącym wymaganiom użytkowników. Wskazuje, że część obrazów jest generowanych wcześniej, ale dla pełnego środowiska jest to niemożliwe (np. cieniowanie, oświetlenie). W praktycznych rozważaniach nad możliwymi zastosowaniami opisanych metod autor wymienia chociażby generowanie wirtualnej rzeczywistości. Stworzone w ten sposób symulowane środowisko, zaczerpnięte właśnie z gier komputerowych, ma już dziś szerokie zastosowania (np. w szkoleniach lub odwzorowaniu miejsc niebezpiecznych dla zdrowia człowieka).

Ostatni rozdział w tym bloku tematycznym dotyczy jednej z najważniejszych technologii stosowanych w oprogramowaniu użytkowym – kompresji danych. Poprawne wdrożenie rozwiązań związanych z tym zagadnieniem umożliwia zapewnienie wydajnego przesyłania informacji przez sieć, tworzenie kopii bezpieczeństwa zajmujących mniej przestrzeni dyskowej lub dużą kompresję wideo (stosowaną powszechnie w telewizji cyfrowej). Na kartach tego rozdziału w przystępny sposób przybliżone zostają zarówno metody stratnego, jak i bezstratnego kodowania informacji (m.in. kodowanie długości serii, metoda słownikowa, kod Huffmana). Szczegółowej analizie zostały poddane sposób zapisu obrazu JPEG oraz standard wideo MPEG-2.

Trzeci blok tematyczny rozpoczyna rozdział *Wyszukiwanie*, który w ciekawy sposób obnaża matematyczne podstawy wyszukiwania danych w dużych zbiorach. Czy jest to dysk komputera, czy sieć – to problemy z szybkim uzyskaniem odpowiedzi na zadane zapytanie w dużym uogólnieniu wydają się podobne. V. A. Spraul w przystępny sposób wyjaśnia, jak

porządkowane są dane, jak tworzy się indeksy oraz wskazuje podstawowe zasady działania algorytmów obsługujących proces wyszukiwawczy. W wyszukiwaniu sieciowym nawiązuje oczywiście do serwisu Google, gdzie przy jego pomocy przywołuje takie zagadnienia, jak klasyfikacja wyników oraz efektywne przeszukiwanie indeksów.

Ciekawym tematem okazuje się współbieżność. Na przykładzie przelewów bankowych wykonywanych na jednym koncie przez dwie osoby autor obnaża problemy mogące wyniknąć z jednoczesnego wykonywaniu takich zadań. Wskazuje także kilka rozwiązań, jak przeprowadzić podobne operacje, by były one zabezpieczone przed przekłamaniami.

Ostatni rozdział *Trasy na mapach* to próba wytłumaczenia sposobu działania systemów informacji geograficznej (GIS). Przedstawione zostały tu algorytmy wyszukiwania najszybszej trasy oraz opisano, jak zapewnić optymalizację ścieżki docelowej składającej się z wielu możliwych punktów pośrednich.

Omówiona publikacja powinna być lekturą obowiązkową każdego entuzjasty nowoczesnych technologii. Stanowi ona dobre wprowadzenie w tematykę bezpieczeństwa informacji, multimediów oraz technologii komunikacyjno-informacyjnych. Atutem, którego nie sposób lekceważyć i który zdecydowanie przemawia za książką A.V. Spraula, jest bogaty aparat pomocniczy w postaci ilustracji, wykresów i tabel, znacznie ułatwiający zrozumienie początkowo sprawiających wrażenie trudnych zagadnień matematycznych. Osoby zainteresowane tematami podjętymi w publikacji niewątpliwie zdobędą cenną wiedzę odnośnie do procedur działania poszczególnych typów aplikacji. Powinny być również usatysfakcjonowane zawartymi w książce licznymi radami praktycznymi oraz próbami przewidzenia dalszego rozwoju omówionych technologii.

Bibliografia

Announcing the ADVANCED ENCRYPTIN STANDARD (AES) [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Black John, Cochran Martin, Highland Trevor, *A Study of the MD5 Attacks: Insights and Improvements* [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: http://www.cs.colorado.edu/~jrblack/papers/md5e-full.pdf.

HTTP Over TLS [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: https://tools.ietf.org/html/rfc2818.

PKCS #1 v2.1: RSA Cryptography Standard [online] [dostęp 31 marca 2017]. Dostępny w World Wide Web: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf.

Spraul V. Anton, *Jak działa oprogramowanie? Tajemnice komputerowych mechanizmów szyfrowania, obrazowania, wyszukiwania i innych powszechnie używanych technologii*, Gliwice 2016.

Should Technological Aspects of ICT Software Be Known only to the Chosen Ones?

Abstract: Not everyone can write a computer program, it seems obvious. However, should people who do not have a technical education know the basic principles of how computer software works? Well, why not? This seemingly difficult task has been taken up by the author of *Jak działa oprogramowanie? Tajemnice komputerowych mechanizmów szyfrowania, obrazowania, wyszukiwania i innych powszechnie używanych technologii.* Based on simple examples known from everyday life, he decided to explain mechanisms of the most popular and interesting computer software.

Keywords: communication and information technology, cyber security, ICT, multimedia.