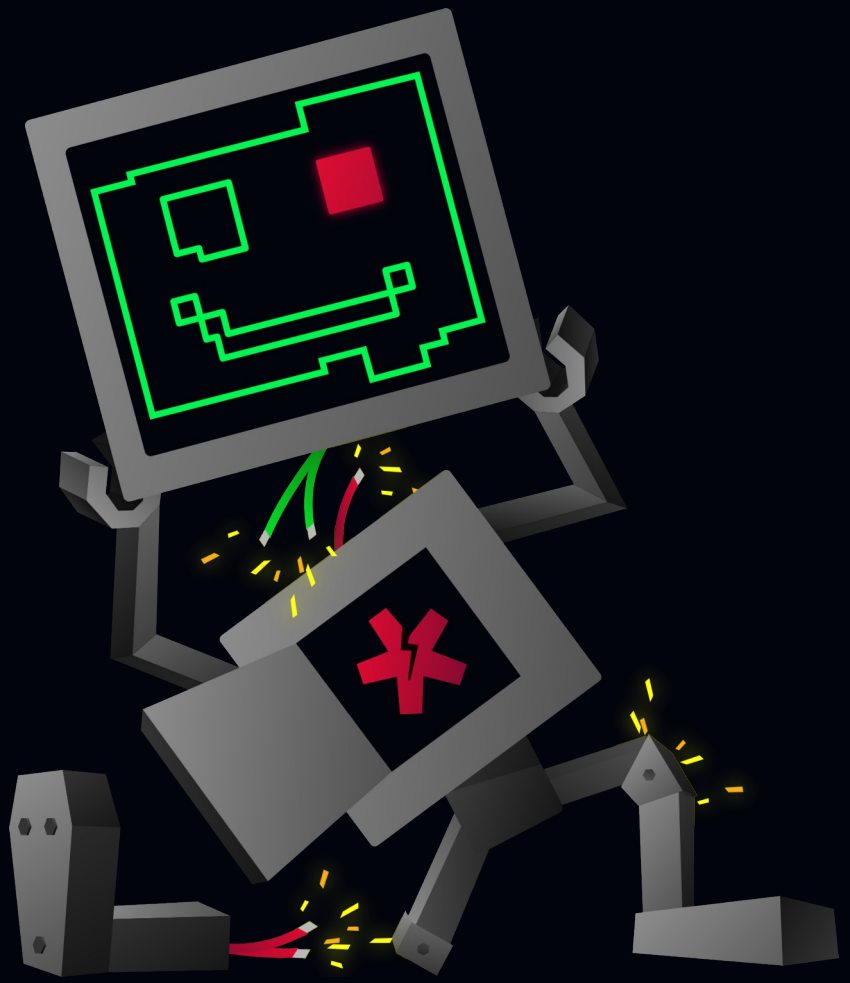
THE H@CK SUMMIT

C:\>

Wyrzucamy algorytm Gutmanna do kosza.



Paweł Kaczmarzyk
Kaleron sp. z o. o.

thehacksummit.com 19-20 października 2023 PGE Narodowy + Online

ORGANIZATORZY:

ACADEMIC PARTNERS

Lektura obowiązkowa

Peter Gutmann:

Secure Deletion of Data from Magnetic and Solid State Memory

https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

Jest to najczęściej cytowany artykuł w kontekście możliwości odzyskania danych po nadpisaniu i podstawa jednego z najpopularniejszych algorytmów nadpisywania danych.

Rodzaje cyfrowych nośników danych

Magnetyczne:
- **dyski twarde**,
- taśmy magnetyczne
- dyskietki

Optyczne:
- CD
- DVD
- Blu-Ray
- HD-DVD

Półprzewodnikowe:
- SSD
- pendrive
- karty pamięci
- eMMC
- inne pamięci wbudowane

Rezystywne:
- PCRAM
- ReRAM
- MRAM
- NanoRAM

Ulotne:
- DRAM
- SRAM

Papierowe:
- karty perforowane
- taśmy perforowane

Standardy regulujące niszczenie danych

AFSSI-5020 (*Air Force System Security Instruction 5020*),

CSEC ITSG-06 (*Communication Security Establishment Canada, Information Technology Security Guide – 06*)

HMG-IS5 (*Her/His Majesty Government Infosec Standard 5*)

IEEE 2883-2022 (Institute of Electrical and Electronics Engineers, *Standard for Sanitizing Storage*),

NAVSO P-5239-26 (*Navy Staff Office Publication 5239-26, Information Systems Security Program Guidelines*),

NISPOM DoD 5220.22-M (*National Industrial Security Program Operating Manual, Departament of Defence 5220.22-M*),

Standardy regulujące niszczenie danych

NIST SP 800-88 (*National Institute of Standards and Technology*, *Guidelines for Media Sanitization*),

NSCS-TG-025 (*National Computer Security Center, Technical Guidelines 025, A Guide to Understanding Data Remanence in Automated Information Systems*),

RCMP TSSIT OST-II (*Royal Canadian Mounted Police, Media Sanitation of the Technical Security Standards for Information Technology*)

VSITR (*Verschlusssachen IT Richtlinien*),

ГОСТ Р50739—95 (*Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования*),

Metody niszczenia danych

Skuteczne:
Po zastosowaniu tych metod danych nie da się odzyskać żadnymi znanymi metodami ani metodami mogącymi powstać w przyszłości. Nie pozwalają na to prawa fizyki

Nieskuteczne:
Jedynie w mniejszym lub większym stopniu utrudniają dostęp do danych. Istnieje fizyczna możliwość odzyskania danych, nawet, jeśli nigdy nie zostanie zrealizowana praktycznie.

Fizyczne:
- mechaniczne,
- chemiczne,
- demagnetyzacja,
- termiczne,
- indukcyjne,
- pirotechniczne.

Programowe:
- kosz systemowy,
- kasowanie w strukturach logicznych,
- formatowanie partycji,
- **nadpisywanie,**
- Secure Erase,
- Block Erase,

Bit w zapisie magnetycznym

„... when a one is written to disk the media records a one, and when a zero is written the media records a zero. However the actual effect is closer to obtaining a 0.95 when a zero is overwritten with a one, and a 1.05 when a one is overwritten with a one.”

„... gdy na dysk zapisana jest jedynka, nośnik rejestruje jedynkę, a gdy zapisywane jest zero, nośnik rejestruje zero. Jednakże rzeczywisty efekt jest bliższy uzyskaniu 0,95 w przypadku nadpisania zera jedynką i 1,05 w przypadku nadpisania jedynki jedynką.”

***P. Gutmann**: Secure deletion …*
Methods of Recovery for Data on Magnetic Media

Kodowanie danych w zapisie magnetycznym

- Sumy kontrolne i kody ECC

- Randomizacja

- Kodowanie RLL

Kodowanie danych w zapisie magnetycznym

1000010001000010 01
0000100010000010 00
1000001000100001 00
0000100010001000 00

Minimalna jednostka adresacji

„...when data is written to the medium, the write head sets the polarity of most, but not all, of the magnetic domains. This is partially due to the inability of the writing device to write in exactly the same location each time, and partially due to the variations in media sensitivity and field strength over time and among devices.”

„...kiedy dane są zapisywane na nośniku, głowica zapisująca ustawia polaryzację większości, ale nie wszystkich, domen magnetycznych. Dzieje się tak częściowo ze względu na brak możliwości zachowania precyzji zapisu za każdym razem dokładnie w tym samym miejscu, a częściowo ze zmian w czułości nośnika i natężeniu pola w czasie i pomiędzy urządzeniami.”

***P. Gutmann**: Secure deletion …*
Methods of Recovery for Data on Magnetic Media

Śledzenie ścieżki

„Deviations in the position of the drive head from the original track may leave significant portions of the previous data along the track edge relatively untouched.”

„Odchylenia położenia głowicy dysku od pierwotnej ścieżki mogą pozostawić znaczne części poprzednich danych wzdłuż krawędzi ścieżki stosunkowo nietknięte.”

***P. Gutmann**: Secure deletion …*
Methods of Recovery for Data on Magnetic Media

Przemagnesowanie warstwy magnetycznej

„When all the above factors are combined it turns out that each track contains an image of everything ever written to it, but that the contribution from each «layer» gets progressively smaller the further back it was made.”

„Kiedy wszystkie powyższe czynniki zostaną połączone, okaże się, że każda ścieżka zawiera obraz wszystkiego, co kiedykolwiek zostało na niej zapisane, ale wkład każdej «warstwy» staje się coraz mniejszy w miarę nadpisywania kolejnych.”

***P. Gutmann**: Secure deletion …*
Methods of Recovery for Data on Magnetic Media

O jeden most za daleko...

„The general concept behind an overwriting scheme is to flip each magnetic domain on the disk back and forth as much as possible (this is the basic idea behind degaussing) without writing the same pattern twice in a row.”

„Ogólna koncepcja schematu nadpisywania polega na odwracaniu każdej domeny magnetycznej na dysku w tę i z powrotem tak bardzo, jak to możliwe (jest to podstawowa idea demagnetyzacji) bez zapisywania tego samego wzoru dwa razy pod rząd.”

***P. Gutmann**: Secure deletion …*
Erasure of Data stored on Magnetic Media

O drugi most za daleko...

„To erase magnetic media, we need to overwrite it many times with alternating patterns in order to expose it to a magnetic field oscillating fast enough that it does the desired flipping of the magnetic domains in a reasonable amount of time. (…) The best we can do is to use the lowest frequency possible for overwrites, to penetrate as deeply as possible into the recording medium.”

„Żeby wymazać nośnik magnetyczny, musimy go wielokrotnie nadpisywać naprzemiennymi wzorami, aby wystawić go na działanie pola magnetycznego oscylującego na tyle szybko, aby w rozsądnym czasie spowodowało to pożądane odwrócenie domen magnetycznych. (…) Najlepsze, co możemy zrobić, to użyć najniższej możliwej częstotliwości do nadpisywania, aby wniknąć najgłębiej, jak to możliwe w nośnik.”

***P. Gutmann**: Secure deletion …*
Erasure of Data stored on Magnetic Media

Kody korekcji ECC

„Therefore even if some data is reliably erased, it may be possible to recover it using the built-in error-correction capabilities of the drive. ”

„Dlatego nawet jeśli niektóre dane zostaną niezawodnie usunięte, możliwe będzie ich odzyskanie przy użyciu wbudowanych funkcji korekcji błędów dysku.”

***P. Gutmann**: Secure deletion …*
Further Problems with Magnetic Media

Konkluzja

„Data which is overwritten an arbitrarily large number of times can still be recovered provided that the new data isn't written to the same location as the original data...”

„Dane, które zostały nadpisane dowolną liczbę razy, można nadal odzyskać, pod warunkiem, że nowe dane nie zostaną zapisane w tej samej lokalizacji, co dane oryginalne...”

***P. Gutmann**: Secure deletion …*
Conclusion

PRML – Partial Response – Maximum Likelihood

„The article*) states that «The encoding of hard disks is provided using PRML and EPRML», but at the time the Usenix article was written MFM and RLL was the standard hard drive encoding technique…”

„W artykule*) stwierdza się, że «Kodowanie dysków twardych odbywa się przy użyciu PRML i EPRML», ale w czasie, gdy pisano artykuł Usenix, standardową techniką kodowania dysków twardych były MFM i RLL...”

*) ***C. Wright, D. Kleiman, R. R. Shyaam Sundhar****: Overwriting Hard Drive Data: The Great Wiping Controversy.*

P. Gutmann*: Secure deletion … Further Epilogue*

Literatura uzupełniająca:

C. Wright, D. Kleiman, R. R. Shyaam Sundhar*: Overwriting Hard Drive Data: The Great Wiping Controversy.*

R. Gomez, A. Adly, I. Mayergoyz, E. Burke*: Magnetic Force Scanning Tunnelling Microscope Imaging of Overwritten Data,*

R. Gomez, E. Burke, A. Adly, I. Mayergoyz, J. Gorczyca*: Microscopic Investigations of Overwritten Data,*

I. D. Mayergoyz, C. Tse*: Spin-stand Microscopy of Hard Disk Data*

С. Р. Коженевський*: Перезапись информации.*

Literatura uzupełniająca:

B. M. Chen, T. H. Lee, K. Peng, V. Venkataramanan: *Hard Disk Drive Servo Systems,*

A. al-Mamun, G. X. Guo, Ch. Bi*: Hard Disk Drive Mechatronics and Control,*

С. Р. Коженевський*: Механика и сервосистема,*

K. A. Schouhamer Immink*: Codes for Mass Data Storage Systems,*

B. Vasić, E. M. Kurtas*: Coding and signal processing for magnetic recording systems*

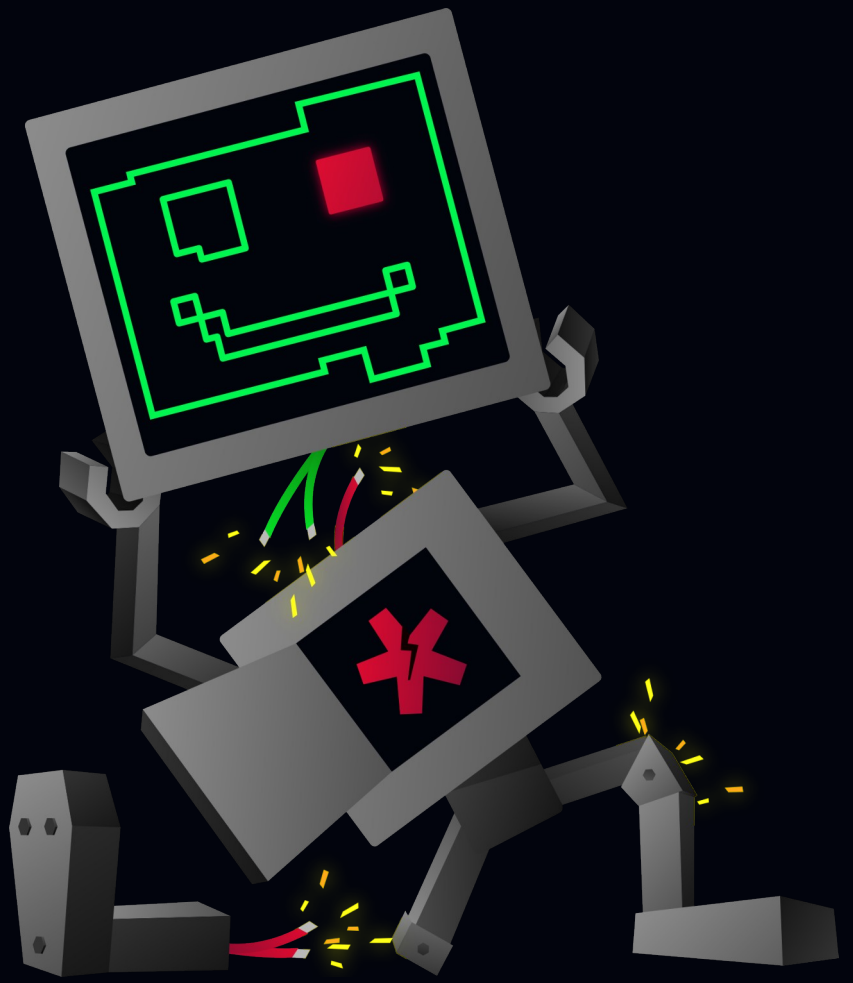
OCEŃ PRELEKCJĘ

Wyrzucamy algorytm Gutmanna do kosza

Paweł Kaczmarzyk

https://thehacksummit.com/user.html#!/lecture/THS23-56fa/rate

THE H@CK SUMMIT



Dziękujemy za uwagę!

Zapraszamy do zadawania pytań oraz oceny wystąpienia pod nagraniem.

thehacksummit.com | 19-20 października 2023 | PGE Narodowy + Online

ORGANIZATORZY:

ACADEMIC PARTNERS

DOWÓDZTWO KOMPONENTU WOJSK OBRONY CYBERPRZESTRZENI