Toruń, 9.05.2022

Analiza oświadczenia prof. Kobusa dla prasy w sprawie wykorzystywania oprogramowania szpiegującego oraz fałszowania wyników egzaminów studentów WFAiIS

Część I

(Nie)możliwość wykorzystania systemów „live”

Profesor Kobus z całą stanowczością oświadcza, że *„nieprawdziwy jest zarzut wymuszania instalacji innego systemu operacyjnego aniżeli ten, który jest zalecany przez producenta”* posiadanego przez studenta komputera osobistego.

Stosując język prof. Kobusa: pan profesor jest fizykiem teoretycznym i logika powinna być czymś znajomym, a jednak wypowiedzi pana profesora sugerują o dziwo, że tak nie jest… Oczywistym jest również, że **cytując wyrwane z kontekstu fragmenty wyciągnięte z wielostronicowych, opublikowanych w Internecie tekstów, prof. Kobus posuwa się do daleko idącej manipulacji.**

Przypomnijmy zatem jaki jest stan faktyczny tej historii. Już w apelu do prorektor ds. studenckich, prof. Beaty Przyborowskiej jasno przedstawiliśmy całą sprawę: **stosowane przez prof. Kobusa oprogramowanie nie działa prawidłowo z systemami typu „live”**. To jest fakt, który **był zgłaszany wielokrotnie przez studentów bezpośrednio do prof. Kobusa.** Ten fakt **był również sygnalizowany prorektor Przyborowskiej** pismami formalnymi **jeszcze przed terminem kolokwium**. Problemy występujące z systemami typu „live” były na tyle istotne, że uniemożliwiały prawidłowe podchodzenie do zaliczania, zatem studenci z obawy przed niezaliczeniem **jedynego podejścia** do kolokwium, które mieli (co już samo w sobie jest naruszeniem zasad panujących na uczelniach wyższych), nie mogli ryzykować zdawania kolokwium na dystrybucjach typu „live”.

Przypomnijmy również, że prof. Kobus dopuszcza do poprawy kolokwium tylko *„wybranych studentów”*, jednak *„z zasady nie organizuje kolokwium poprawkowego, bo nie ma takiej potrzeby”*, lub ewentualnie organizuje je *„tylko w sytuacji, kiedy np. choroba komuś nie pozwoliła podejść do kolokwium”*… To wszystko są oczywiście cytaty z udokumentowanych wiadomości mailowych prof. Kobusa wysyłanych do studentów, które przytaczaliśmy już w naszym apelu.

W związku z powyższym, **studenci mając tylko jedną szansę** na zaliczenie kolokwium **zmuszeni są do eliminacji błędów, które mogą pojawić się w niepewnie działającym skrypcie wątpliwego pochodzenia**, który – powiedzmy wprost – **nie został dopuszczony do przeprowadzania zaliczeń przez podmioty uczelni właściwe do analizy takiego oprogramowania.** Przypomnijmy również, że systemem egzaminacyjnym dopuszczonym do stosowania wśród nauczycieli akademickich na uczelniach wyższych w całej Polsce jest system Moodle, z którego korzysta oczywiście również wielu pracowników UMK.

Dowody występowania przeróżnych problemów z systemami typu „live” prof. Kobus sam umieścił w opisie własnego skryptu ssctl, skutecznie tym samym odstraszając studentów do korzystania z tego typu rozwiązań. Zacytujmy zatem jeden z problemów, na które zwraca uwagę egzaminator oraz sposób jego rozwiązania:

Sprawdziłem, że w przypadku użycia dystrybucji Fedora-Workstation-Live-x86_64-35 domyślnie uruchamiane jest interfejs graficzny Gnome, które korzysta z protokołu Wayland. **Niestety, w takim środowisku nie działa komenda import z pakietu ImageMagick, więc nie zadziała skrypt ssctl.**

Rozwiązanie problemu wymaga wykonania następujących kroków:

- przelogowania się na konto superużytkownika

  # sudo su - root

- zainstalowania potrzebnych pakietów

  # dnf -y install ImageMagick bind-utils

(Ten sam efekt można uzyskać przy pomocy komendy './ssctl install'.)

- utworzenie dodatkowego konta użytkownika (np. so),

  # useradd so

  # passwd so

- przelogowania się na konto nowoutworzonego użytkownika so (w górnym prawym rogu trzeba wybrać "Power Off/Log Out", a następnie "Switch user")

- na ekranie logowania, po podaniu identyfikatora nowego użytkownika i hasła, ale przed zatwierdzeniem hasła, należy najechać myszą na zębatkę (w prawym dolnym rogu) i wybrać "GNOME on Xorg"

Źródło: https://jkob.fizyka.umk.pl/so+sk/ssctl

Oczywiście takich problemów jest więcej a przy każdorazowym uruchomieniu komputera kroki naprawcze, jak te wymienione powyżej, należy wykonywać ponownie. Podnosiliśmy to również w apelu wskazując, że **systemy typu „live” nie nadają się do przeprowadzania tego typu zaliczeń** z uwagi na brak zapisywania postępu pracy studenta oraz właśnie z powodu konieczności instalacji zależności wymaganych przez skrypt wykładowcy za każdym razem, gdy nastąpi ponowne uruchomienie komputera. **Zadziwiającym jest, że prof. Kobus, który od lat wykłada materiał związany z systemami klasy Linux za wszelką cenę stara się udowodnić opinii publicznej, że nie rozumie problemów pojawiających się w przypadku użycia dystrybucji „live”.**

Co więcej, w treści swojego skryptu, będącego jednocześnie instrukcją użytkowania, sam egzaminator sugeruje, że *„w zeszłym roku jeden ze studentów rekomendował użycie dystrybucji »elementary OS«”* oraz że na tym systemie **skrypt „powinien” działać…** I tu pojawia się pytanie: **czy prof. Kobus rzeczywiście sprawdzał jakikolwiek system typu „live”, czy jego instrukcja oraz wygłaszane sądy opierają się tylko na domysłach?** Brak wiedzy na temat istotnych problemów z systemami typu „live” sugeruje, że **prof. Kobus nie ma doświadczenia w korzystaniu z tego typu dystrybucji**, co akurat wiele by wyjaśniało.

Przypomnijmy raz jeszcze, że oprogramowanie stosowane przez prof. Kobusa nie zostało oficjalnie zatwierdzone do przeprowadzania zaliczeń przez podmioty funkcjonujące na uczelni odpowiedzialne za analizę takiego oprogramowania, a zatem studenci obawiający się korzystania z tego typu podejrzanego skryptu mają słuszne obawy, że może ono działać w nieprawidłowy sposób, co uniemożliwi im podejście do jedynego kolokwium przesądzającego o dopuszczeniu do egzaminu, a tym samym do niezaliczenia roku studiów.

Zwróćmy uwagę na jeszcze jeden aspekt. **To, że system nie jest wspierany przez producenta oprogramowania oznacza zarówno brak wsparcia w przypadku instalacji systemu na dysku twardym, jak i uruchomienia systemu typu „live" z pendrive'a.** Czy może prof. Kobus sądzi, że w przypadku uruchomienia dystrybucji „live" magicznie tworzą się nowe podzespoły wewnątrz komputera z magicznie przystosowanymi sterownikami do systemu Linux, lub też producent sprzętu nagle zmienia zdanie co do wspieranych systemów operacyjnych jego urządzenia? To jest kolejna obserwacja, która sprawia, iż mamy obawy co do doświadczenia prof. Kobusa z systemami typu „live". **Wypowiedzi egzaminatora sugerują bowiem zaskakująco małą wiedzę w tym temacie, szczególnie jak na osobę prowadzącą przedmiot „systemy operacyjne" czy „sieci komputerowe" od wielu lat.**

Powstaje zatem pytanie, czy prof. Kobus ma odpowiednie kwalifikacje do nauczania koordynowanych przez siebie przedmiotów? Jak wiemy wykładowca pracuje w Katedrze Mechaniki Kwantowej jako fizyk teoretyczny. Co więcej, na wydziale wśród fizyków przeprowadzane były egzaminy kwalifikacji nauczania informatyki, z uwagi na zbyt małe obciążenia dydaktyczne przedmiotami z fizyki, a tym samym konieczność przydzielania fizykom przedmiotów informatycznych. Czy prof. Kobus rzeczywiście wykazał się na nich odpowiednim poziomem wiedzy? Oczywiście tego typu informacji nie udzielą nam władze dziekańskie, które od dawna zatają nadużycia prof. Kobusa, ale z pewnością poprosimy komisje akredytacyjne oraz Ministerstwo Edukacji i Nauki o sprawdzenie tych kwestii.

Oprogramowanie (nie)szpiegujące

Profesor Kobus w swoim oświadczeniu twierdzi, że dostarczany przez niego skrypt ssctl *„nie jest programem szpiegującym, ale programem o otwartym kodzie służącym do przeprowadzania kolokwiów i egzaminów w trybie zdalnym"*.

Zacznijmy od tego, że **oprogramowanie jest autorskim skryptem napisanym przez prof. Kobusa, który zawiera niesprawdzone przez odpowiednie podmioty funkcjonalności**, a przede wszystkim nie zostało dopuszczone do przeprowadzania zaliczeń na uczelni, jak wyjaśnialiśmy już wcześniej. Ponadto studenci od lat skarżą się, że **oprogramowanie to nie działa prawidłowo**, o czym wspominaliśmy wyżej oraz w apelu do prorektor Przyborowskiej. Sam prof. Kobus przyznał przecież na nagraniu z kolokwium, że właśnie podczas odbywania zaliczenia pojawiły się *„dziwne"* problemy z wykorzystywanym oprogramowaniem. Co do tego nie ma zatem żadnych wątpliwości.

Profesor Kobus: *„(…) Jakieś tutaj dziwne rzeczy się dzieją"*

Nagranie: https://drive.google.com/file/d/1BRqfsOOC7vH5O1zaRQdXQkEJ-6DEUCvr/view?usp=sharing

---

Co jest jednak najbardziej istotne, **definicja oprogramowania szpiegującego (ang. „spyware") nie opiera się na rozróżnieniu, czy program jest w postaci otwartego kodu, czy nie.** Nie byłoby po prostu możliwe określenie, że każdy kod jawny musi być kodem bezpiecznym, gdyż nawet takie programy mogą zawierać celowe luki bezpieczeństwa, czy wykradać dane użytkowników.

Przykładowo niedawna afera z otwarto źródłowym oprogramowaniem Audacity pokazuje, że nic nie stoi na przeszkodzie, aby w programie o otwartym kodzie znalazły się funkcjonalności pozwalające na wykradanie danych osób, korzystających z takich programów:

https://www.instalki.pl/aktualnosci/software/48627-audacity-spyware.html

Oczywiście tego typu przypadków jest całe mnóstwo, wystarczy choć trochę zainteresować się tematem, od czego przede wszystkim powinien zacząć prof. Kobus nim przedstawił swoje kuriozalne stanowisko.

Podkreślmy zatem, iż **to cel użycia oprogramowania jest istotny w określeniu, czy oprogramowanie jest szkodliwe, a nie kwestia otwartości kodu.** Gdyby było inaczej, wówczas programy takie jak chociażby bardzo popularny framework Metasploit, czyli narzędzie do łamania zabezpieczeń systemów informatycznych (w szczególności zawierający dużą bazę gotowych exploitów), nie mogłoby być upubliczniane na GitHubie z powodu naruszenia prawa. Tak jednak nie jest, bo to właśnie przeznaczenie wykorzystania oprogramowania jest istotne a nie jawność jego kodu (w przypadku legalnego użycia narzędzia Metasploit będziemy mówić o testach penetracyjnych). Na GitHubie jest nawet cała kategoria programów otwarto źródłowych oznaczonych hasztagiem #spyware:

https://github.com/topics/spyware

Znajdziemy tam chociażby takie oprogramowanie jak: AdoBot, BlackMamba, Trojan Cockroach, StupidKeylogger, Richkware etc. Cały ten software może zostać wykorzystany w sposób sprzeczny z prawem, co nie znaczy że nie mamy wglądu do kodu tego oprogramowania.

Podobnie będzie ze skryptem prof. Kobusa – **to, że jest to oprogramowanie o otwartym kodzie źródłowym nie wyklucza bycia oprogramowaniem szkodliwym.** Dlatego przede wszystkim należy odnieść się do definicji słowa „spyware" oraz cech programu, które musi ono spełniać. W liście otwartym do dra Tomasza Wolniewicza, dyrektora Uczelnianego Centrum Informatycznego (który de facto nie raczył na ten list odpowiedzieć – tak niestety „dba się" o bezpieczeństwo studentów na UMK) tłumaczyliśmy bardzo dokładnie, jakie cechy skryptu ssctl wskazują na fakt bycia oprogramowaniem szpiegującym.

Link do listu: https://drive.google.com/file/d/1W1YfwHSKPXCCjh8c8tgayDgNlhiBRp_G/view?usp=sharing

---

Przypomnijmy, że **zgodnie z definicją o oprogramowaniu szpiegującym mówimy, gdy umożliwia ono dostęp pewnej osobie do poufnych informacji o jakiejś innej osobie lub jej aktywności na komputerze, bez jej wiedzy lub bez jej zezwolenia.** Definicja nie odnosi się zatem do tego, czy oprogramowanie dostępne jest w postaci jawnego kodu czy nie. Istotne z punktu widzenia definicji jest przeznaczenie oprogramowania oraz użycie go bez wiedzy lub zgody użytkownika.

Tu natomiast nie ma żadnych wątpliwości – **oprogramowanie było użyte w celu wykradania poufnych danych o systemach operacyjnych studentów, w tym poufnego identyfikatora systemu związanego stricte z prywatnością użytkownika.** Ponadto za pomocą oprogramowania prof. Kobus wykonywał bardzo dużą liczbę zrzutów ekranu w celu śledzenia aktywności użytkownika na komputerze. Zrzuty ekranów nie były w żaden sposób kontrolowane ani cenzurowane, a zatem mogło dochodzić do uwieczniania na nich danych osobowych w różnej postaci, od adresów mailowych czy loginów zapisanych w zakładkach przeglądarki oraz na stronach wyszukiwarki, przez prywatne dane zapisane na pulpicie czy plikach na koncie wydziałowym, aż po hasła logowania do różnych systemów (poczta, konto Google etc.). **Skąd pewność prof. Kobusa, że na dziesiątkach tysięcy zrzutów ekranu nie ma żadnych danych osobowych?** Z pewnością odpowiednie organy nadzoru zainteresują się tą sprawą, a na pewno takie doniesienie studenci będą składać.

Przypomnijmy, że w liście otwartym do dra Wolniewicza tłumaczyliśmy, że **studenci w sposób bardzo stanowczy nie godzili się na korzystanie ze skryptu podczas odbywania kolokwium, czego naturalną koleją rzeczy było złożenie skarg formalnych do władz rektorskich oraz innych**

podmiotów na UMK (w tym również do dra Wolniewicza, który wtedy także nie zareagował – taki już mamy poziom bezpieczeństwa na UMK). Przypomnijmy również, że **to właśnie z powodu protestu studentów w sprawie wątpliwego oprogramowania władze rektorskie wyraziły zgodę na przeprowadzenie zaliczenia w sposób stacjonarny,** pomimo obowiązywania zarządzenia Nr 11 rektora UMK z dnia 25 stycznia 2022 nakazującego przeprowadzenie wszystkich zaliczeń sesji zimowej 2021/22 *„z wykorzystaniem metod i technik kształcenia na odległość”*.

Link do zarządzenia:
https://www.umk.pl/koronawirus/organizacja-zajec-dydaktycznych-oraz-dzialalnosc-naukowa/ZR.11.2022.pdf

---

Ponadto, wbrew temu co prof. Kobus twierdzi, **studenci nie byli informowani o tym, jakie dane zbierane są przez jego autorski skrypt, a tym bardziej w jaki sposób te dane są przetwarzane.** W szczególności **wykładowca nie poinformował studentów o zbieraniu danych w postaci informacji o systemie, czy identyfikatorze znajdującym się w pliku `/etc/machine-id`, który zgodnie z dokumentacją systemu Linux jest daną poufną i nie może być przesyłany przez sieć.** Ponieważ skrypt prof. Kobusa miał być uruchamiany na prywatnych komputerach studentów, które nie były systemami typu „live” – gdyż te nie współpracują poprawnie ze skryptem ssctl – identyfikator `/etc/machine-id` mógł zostać wykorzystany do śledzenia aktywności studentów w Internecie.

Profesor Kobus w swoim oświadczeniu zdaje się jednak kwestionować nawet poprawność dokumentacji systemu Linux twierdząc, że *„plik /etc/machine-id nie ma charakteru poufnego”*. Pytanie zatem brzmi, czy to wynika z tak wielkiej wiedzy o systemie, czy może jednak braku odpowiednich kompetencji? Przypomnijmy, co na ten temat mówi dokumentacja:

`This ID` **`uniquely identifies`** `the host. It should be considered` **`"confidential", and must not be exposed in untrusted environments, in particular on the network`**`. If a stable unique identifier that is tied to the machine is needed for some application, the machine ID or any part of it must not be used directly.` **`Instead the machine ID should be hashed with a cryptographic, keyed hash function, using a fixed, application-specific key.`**

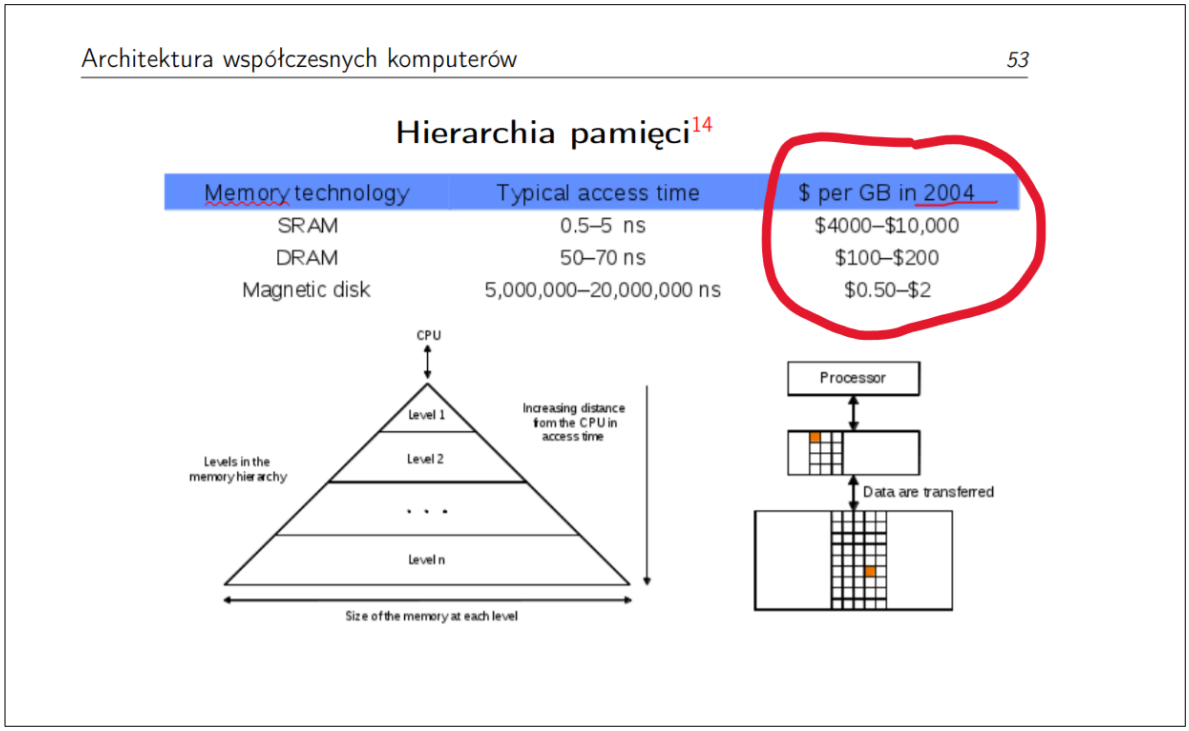
Źródło: https://man7.org/linux/man-pages/man5/machine-id.5.html

---

Zatem **dokumentacja systemu Linux wprost określa plik `/etc/machine-id` jako poufny,** a do tego tłumaczy, w jaki sposób można używać wartości zapisanej w tym pliku, gdy jest ona z jakiegoś powodu potrzebna. Należy w takiej sytuacji skorzystać z kryptograficznych funkcji skrótu, które używa się m.in. do przechowywania haseł w bazach danych. Ni mniej ni więcej oznacza to, że **dokumentacja systemu Linux bezpośrednio sygnalizuje jak skrajnie poufną informacją o systemie jest ten identyfikator, sugerując wręcz konieczność zabezpieczania jej za pomocą funkcji stosowanych w kryptografii, które z definicji muszą gwarantować największe możliwe bezpieczeństwo.**

Ponieważ prof. Kobus w swoim oświadczeniu wykazuje się niezwykłą arogancją (co oczywiście studenci znają doskonale z zajęć oraz zaliczeń), pozostaje nam jedynie zaproponować, aby wykładowca zaczął sam spisywać własną dokumentację systemu Linux oraz umieścił ją w swoich archaicznych notatkach. Już w tej chwili na wykładach prof. Kobusa studenci uczą się tak niezmiernie przydatnych kwestii jak kosztu pamięci w roku 2004, czy pozycji superkomputerów na liście top500 na

kilka lat wstecz. Taka „nowa” dokumentacja z pewnością będzie doskonałym uzupełnieniem niepotrzebnej wiedzy przekazywanej studentom Informatyki Stosowanej na WFAiIS.



Zwrócimy również uwagę na jeden bardzo istotny szczegół. Mianowicie **prof. Kobus, prawdopodobnie celowo, całkowicie pomija fakt, że ostateczną wersję skryptu używanego na kolokwium studenci otrzymują na chwilę przed rozpoczęciem tegoż zaliczenia.** Przypomnijmy, że kolokwium, o którym pisaliśmy w apelu odbyło się 1 lutego 2022, zaś ostatnia zmiana w kodzie skryptu datowana jest na 31 styczeń 2022 (jest to data wpisana w treść skryptu przez prof. Kobusa). **Studenci nie mają zatem możliwości zapoznania się z rzeczywistym działaniem skryptu przed odbyciem zaliczenia, bo egzaminator nie udostępnia go w ostatecznej formie wystarczająco wcześnie, wbrew temu co próbuje sugerować opinii publicznej.**

Przypomnijmy również, że **sposób zbierania i przetwarzania danych studentów przez prof. Kobusa stoi w sprzeczności z RODO,** co również podkreślaliśmy w liście otwartym do dra Wolniewicza. Zgodnie z zapisami ogólnego rozporządzenia o ochronie danych klauzula informacyjna dotycząca przetwarzania danych powinna być zwięzła, przejrzysta, zrozumiała oraz podana w łatwo dostępnej formie, jasnym i prostym językiem. **Twierdzenie, że skrypt jest oprogramowaniem o otwartym kodzie źródłowym, co rzekomo wypełnia obowiązek informacyjny jest błędem i wskazuje na niezgodność z przepisami prawa, a wręcz na ich nieznajomość.** Jest to tym bardziej zaskakujące, gdyż wszyscy pracownicy UMK w roku 2021 mieli obowiązek odbycia szkolenia pn. „Nowe podejście do ochrony danych osobowych po wejściu RODO”.

Dlaczego zatem prof. Kobus stosując od dłuższego czasu podobne oprogramowanie nigdy nie zadbał o poinformowanie studentów, w jaki sposób ich dane będą przetwarzane? Odpowiedź sama nasuwa się na myśl: po prostu legalność oprogramowania nigdy nie była w sferze zainteresowania wykładowcy prawdopodobnie z powodu protegujących prof. Kobusa władz dziekańskich. Przy tak silnym wsparciu osób kierujących wydziałem nie trzeba przecież się martwić o takie szczegóły. Skoro władze dziekańskie posuwają się do naruszania podstawowych praw studentów danych regulaminem

studiów UMK w celu ukrycia fałszowania wyników egzaminów, to tym bardziej kwestie prawne związane z RODO nie powinny martwić pana profesora.

Przypomnieć trzeba również, że w listopadzie 2020 prorektor Przyborowska przekazała za pośrednictwem dra Wolniewicza **wszystkim nauczycielom akademickim na UMK** informację, iż **jedynymi danymi studentów, które nauczyciel akademicki może przetwarzać są numery albumów, gdyż *„umożliwiają one jednoznaczną identyfikację osoby”*.** Dlaczego te wytyczne nie są zatem stosowane w odniesieniu do wymysłów prof. Kobusa? Z pewnością zasugerujemy władzom rektorskim oraz odpowiednim podmiotom nadzoru pracy uczelni skierowanie wykładowcy na ponowny kurs z ochrony danych osobowych, ale czyż to nie władze rektorskie powinny same dbać o tak istotne kwestie prawne na uczelni wyższej? Niedopuszczalnym przecież jest, aby wykładowca uniwersytetu – mianowany profesorem uczelni przez samego rektora UMK – nie posiadał podstawowej wiedzy na temat ochrony danych osobowych pracując rokrocznie z tak liczną grupą studentów.

W swoim oświadczeniu prof. Kobus twierdzi ponadto, że *„zrzuty ekranu służą temu samemu, co obserwacja stanowisk komputerowych w czasie zaliczenia, które odbywa się w pracowni komputerowej”*. Po pierwsze zauważmy, że obserwacja stanowisk nie uwiecznia pulpitu, czy paska zakładek w przeglądarkach uruchomionych na komputerach osobistych studentów, gdzie przecież mogą znajdować się różne dane osobowe, chociażby w postaci adresów mailowych kont prywatnych, loginów czy innych danych, które mogą zostać utrwalone w przypadku wykonywania tysięcy zrzutów ekranu. Ponadto **obserwacja stanowisk nie powoduje <u>rozpowszechniania</u> zrzutów ekranów oraz informacji o systemach operacyjnych i poufnych identyfikatorach `/etc/machine-id` z prywatnych komputerów studentów <u>wśród setek pracowników i studentów wydziału</u>, co praktykował prof. Kobus od co najmniej kilku lat.** Porównanie jest zatem kompletnie nietrafione, gdyż w przypadku obserwacji studenta przy stanowisku komputerowym nie dochodzi do naruszenia jego podstawowych praw obywatelskich.

Co więcej, mając na uwadze nagranie z kolokwium, które prof. Kobus udostępnił studentom, można podejrzewać, że cel zbieranych zrzutów ekranu jest jednak zupełnie inny niż to co sugeruje wykładowca w swoim oświadczeniu. Już w apelu do prorektor Przyborowskiej wskazywaliśmy zamiłowanie egzaminatora do „podglądania” osobistych komputerów studentów, do czego sam prof. Kobus przyznawał się przed prodziekanem ds. kształcenia, prof. Jackiem Jurkowskim.

Profesor Kobus: *„(…) W związku z tym ja już mogę sobie **podejrzeć** (…) Jeśli mogę sobie **podejrzeć**, czy ktoś kto rozwiązywał te zadania (…) Można z grubsza się zorientować, jak to wyglądało, można **podejrzeć** (…) No i teraz w związku z tym oni siedzą, ja mogę **zobaczyć** mhm (…) W związku z tym ja sobie to mogę potem **obejrzeć**, wyświetlić w przyspieszonym tempie (…)”*

Nagranie: https://drive.google.com/file/d/1dRWITEQvNqmk_B2R2K-LcDAqC_DjRzX-/view?usp=sharing

---

Zwróćmy również uwagę na fakt, że prof. Kobus nie tylko rozpowszechniał dane wykradzione z komputerów prywatnych studentów, ale również **udostępnił trzygodzinny zapis wideo z kolokwium, na którym – jak pamiętamy – wymagał od studentów, ażeby mieli *„gęby podoświetlane jak należy”*.** Przy okazji zadziwiające jest, że w tak długim oświadczeniu prof. Kobusa nie znalazł się ani jeden fragment tłumaczący niezwykłą pogardę w stosunku do studentów. Czy może ta pogarda z jaką odnosił się wykładowca do swoich studentów jest również podyktowana tym, że prof. Kobus *„przez cały okres kariery zawodowej zawsze miał na uwadze dobro studentów”*? Brzmi to co najmniej surrealistycznie…

Profesor Kobus: *„No i, no i tyle no… Teraz, wymusiłem na nich, żeby mieli te gęby podoświetlane jak należy, bo tak czasami jest, że nie widzisz człowieka, a jak on jest naświetlony prawidłowo…”*

Nagranie: https://drive.google.com/file/d/1pcQ3n0IvEA7qB1A7WfunhrGRARAweIpL/view?usp=sharing

---

Zauważmy, że w świetle przepisów prawa wizerunek jest również daną osobą, a zatem podlega przepisom o ochronie danych osobowych. Jednakże **prof. Kobus nie miał najmniejszego problemu z udostępnieniem wizerunku wszystkich studentów przystępujących do kolokwium szerokiemu gronu studentów zapisanych na prowadzony przez siebie przedmiot.** Oczywiście prof. Kobus o zgodę nigdy nie pyta, czy to chodzi o wizerunek studenta, czy o zrzuty ekranu prywatnych komputerów osobistych, czy też o poufny identyfikator systemu związany bezpośrednio z prywatnością studenta w przestrzeni internetowej.

Pan profesor twierdzi również, że po zakończonym procesie oceniania studentów dane zbierane przez jego oprogramowanie są usuwane. W świetle powyższych informacji nasuwa się pewne pytanie: czy w ten „proces oceny” wliczają się wszystkie lata studiów, na których studenci podchodzą co roku ponownie do tych samych dwóch zaliczeń u prof. Kobusa aż do momentu napisania pracy inżynierskiej i… zmiany uczelni na inną z powodu blokowania ich przez pana egzaminatora? Wiemy przecież, że dane zbierane w roku akademickim 2020/21 z przedmiotu „systemy operacyjne” były dostępne dla wszystkich studentów i pracowników wydziału WFAiIS co najmniej do dnia, w którym opisywaliśmy to w naszym przeglądzie naruszeń datowanym na 9 lutego 2022.

Jakby nie było, to jednak **przez cały rok kalendarzowy wszyscy użytkownicy systemu wydziałowego mieli nieograniczony dostęp do wszystkich tych danych rzekomo usuwanych po wystawieniu oceny.** Tego typu oświadczenia prof. Kobusa stanowią całkowitą kompromitację nie tylko reprezentowanego przez siebie stanowiska nauczyciela akademickiego, ale również **dyskredytują wszelkie informacje podawane opinii publicznej, nie pozostawiając cienia złudzenia, iż przekazywane mediom kwestie oparte są na manipulacji, obłudzie i zakłamaniu.**

Przegląd naruszeń w oprogramowaniu prof. Kobusa:
https://drive.google.com/file/d/15ivFJRbAQJo_ASUrJks07AXMroDOcLGI/view?usp=sharing

---

W swoim oświadczeniu prof. Kobus twierdzi dodatkowo, że w jego autorskim oprogramowaniu wystarczy usunąć wiersze odpowiedzialne za wykradanie poufnych plików, co nie będzie miało wpływu na funkcjonalność skryptu. **To już musi być żart, bo jak inaczej odbierać nakłanianie studentów do oszukiwania oprogramowania przeznaczonego *„do przeprowadzania kolokwiów i egzaminów w trybie zdalnym”*?** Ponadto, czy studenci mają być rzeczywiście sami odpowiedzialni za zadbanie o swoją prywatność i ochronę danych przez usuwanie fragmentów kodu oprogramowania dostarczanego im na chwilę przed rozpoczęciem zaliczenia? **Czy naprawdę przy takim podejściu autora skryptu ktoś jeszcze ma wątpliwości, że oprogramowanie nie jest oprogramowaniem szpiegującym?** Czy w ogóle prof. Kobus upoważnił kiedykolwiek studentów do jakiejkolwiek modyfikacji skryptu na odbywających się zaliczeniach? My znamy zupełnie odmienne historie, w których studenci otrzymywali oceny negatywne w wyniku wadliwie działającego skryptu…