Systemy operacyjne 2016

Lista zadań nr 11

Na zajęcia 2 lutego 2017

Należy przygotować się do zajęć czytając następujące rozdziały książek:

- Stallings (wydanie ósme): 15.1 – 15.3, 15.5
- Tanenbaum (wydanie czwarte): 7.2 – 7.6, 9.2 – 9.4, 9.6, 9.7

UWAGA! W trakcie prezentacji rozwiązań należy zdefiniować i wyjaśnić pojęcia, które zostały oznaczone **wytłuszczoną** czcionką.

Zadanie 1. Rozważmy **maszynę wirtualną** działającą pod kontrolą **hipernadzorcy** (ang. *hypervisor*). Jaką technikę wykorzystuje się do przetwarzania **instrukcji wrażliwych**? Podaj przykłady instrukcji wrażliwych, które nie są **instrukcjami uprzywilejowanymi**. Jakie problemy rozwiązuje **parawirtualizacja**? Czemu należy zmodyfikować jądro systemu operacyjnego by z niej skorzystać? Podaj podobieństwa i różnice między hipernadzorcą, a warstwą abstrakcji sprzętu i mikrojądrem.

Zadanie 2. Pod kontrolą **hipernadzorcy typu 2** uruchamiamy maszynę wirtualną z systemem operacyjnym bez wsparcia dla parawirtualizacji. Uzasadnij, że w takim przypadku nie można bezpośrednio tłumaczyć adresów wirtualnych gościa, tj. generowanych przez procesy działające pod kontrolą systemu gościa, na adresy fizyczne systemu gospodarza. Jak rozwiązać ten problem programowo, tj. z użyciem **tablic stron-cieni** (ang. *shadow page tables*), a jak sprzętowo, tj. z użyciem **zagnieżdżonych tablic stron** (ang. *nested page tables*)?

Zadanie 3. Kiedy sumarycznie przydzielamy maszynom wirtualnym więcej zwirtualizowanej pamięci fizycznej niż posiada gospodarz, to mówimy o **nadprzydziale pamięci** (ang. *memory overcommitment*). W takiej sytuacji może powstać problem z wydajnością wymiany stron na dysk – opisz go. Jak technika zwana **balonikowaniem** rozwiązuje ten problem?

Rozważmy hipernadzorcę pod którym uruchomiono wiele maszyn wirtualnych z tym samym systemem operacyjnym. Izolacja pamięci operacyjnej między gośćmi prowadzi tu do niepotrzebnego powielania ramek – dlaczego? Jak temu zaradzić używając techniki **deduplikacji ramek**?

Zadanie 4. Zdefiniuj pojęcia **domeny**, **uprawnień** i **macierzy ochrony** w kontekście kontroli dostępu do zasobów. Wyjaśnij różnice między następującymi klasami mechanizmów kontroli dostępu: **DAC** (ang. *discretionary access control*), **MAC** (ang. *mandatory access control*) i **RBAC** (ang. *role-based access control*). Pobieżnie opisz następujące mechanizmy: grsecurity[1], ACL[2] i capsicum[3] – po czym zakwalifikuj je do jednej z powyższych klas. Odpowiedź uzasadnij.

[1] `https://en.wikibooks.org/wiki/Grsecurity/Overview`
[2] `https://www.freebsd.org/doc/en/books/handbook/fs-acl.html`
[3] `https://lwn.net/Articles/482858/`

Zadanie 5. Czym różni się **autoryzacja** od **uwierzytelniania**? Rozważmy system bibliotek **PAM** (ang. *Pluggable Authentication Module*) opisany w podręczniku `PAM(7)`. Na podstawie programu `login` wytłumacz jakie funkcje pokrywają fazy `account`, `auth`, `password`, `session`. Odpowiedz na następujące pytania:

- jak odrzucić użytkownika, który próbuje się zalogować poza godzinami pracy?
- jak umożliwić dostęp do systemu na podstawie **danych biometrycznych**?
- jak wymusić zmianę hasła, które jest starsze niż 180 dni?
- jak w trakcie logowania odszyfrować katalog domowy użytkownika?

Zadanie 6. Przedstaw dwie najpopularniejsze techniki ataków przez wykorzystanie luk w oprogramowaniu – **przepełnienia bufora** (ang. *buffer overflow*) i **programowanie przez powroty** (ang. *return oriented programming*). Wyjaśnij na przykładzie jak atakujący może wykorzystać powyższe techniki do przechwycenia kontroli nad atakowanym programem. Opisz metodę wykrywania błędów przepełnienia bufora z użyciem kanarków (ang. *stack canaries*).

Zadanie 7. Jądro systemu może zapobiegać atakom wymienionym w poprzednim zadaniu dzięki implementacji **zapobiegania wykonywaniu danych** (ang. *Data Execution Prevention*) i generowaniu **losowego układu przestrzeni adresowej** (ang. *Address Space Layout Randomization*). Wyjaśnij zasadę działania powyższych zabezpieczeń. Podaj niezbędne zmiany w oprogramowaniu i sprzęcie, które należy wprowadzić celem ich implementacji. Jak obejść takie zabezpieczenia?

Zadanie 8. System operacyjny może wspomagać wykrywanie niektórych ataków dzięki prowadzeniu **dzienników audytu** (ang. *audit log*), np. z użyciem demona `syslogd(8)`. Z uprawnieniami administratora zajrzyj do katalogu `/var/log` – jakie informacje przechowują pliki dzienników, które można tam znaleźć? Wyjaśnij w jaki sposób może z nich skorzystać oprogramowanie **systemu wykrywania intruzów** (ang. *Intrusion Detection System*). Jakie inne techniki może stosować `IDS`?