

堅

Katashi

Media Asset Management / Zabezpieczanie Gier Flash Media Server

Zabezpieczanie gier FMS/RTMPE

Przedstawiamy propozycję nowatorskiego rozwiązania, którego zadaniem jest zabezpieczanie przesyłania wyników gier, ważnych informacji oraz danych osobowych wraz z systemem weryfikacji i zapisu przebiegu interakcji w czasie rzeczywistym.

Problem

W trakcie naszych obserwacji myśląc o budowie odpowiedniego narzędzia zauważyliśmy, iż na ataki są narażone praktycznie wszystkie aplikacje przesyłające informacje w technologii Klient-Serwer. Szczególnie dotyczy to aplikacji konkursowych, w których występują cenne nagrody – to bowiem motywuje potencjalnych oszustów do łamania zabezpieczeń. Z gruntu większość oszustw jest do wykrycia, jednakże nie wszystkie, a co więcej zmusza to administratorów i operatorów do prowadzenia weryfikacji wyników, co niejednokrotnie sprowadza się aż do testowania rezultatów w bazach danych. Z naszego punktu widzenia jest to czas stracony.

Metody oszustw są różnorakie. Dekompilacja kodu SWF jest pierwszym krokiem na drodze do fałszerstwa. Kolejnym etapem jest wytwarzanie algorytmów, które imitują oryginalny plik SWF, kolejnym wysyłanie wyników na serwer poprzez obserwację transmisji (połączeń), np. via FireBug lub FlashBug.

Ze względu na to podjęliśmy próbę przygotowania takiego narzędzia, którego filozofia działania jest zasadniczo inna.

Rozwiązanie

Nasze rozwiązanie oparte jest o komunikację z użyciem serwera Flash Media Server przy użyciu różnorodnych algorytmów i funkcji zabezpieczających wysyłanie wyników i monitorowanie przebiegu gry lub wydarzenia (np. testów kontrolnych lub egzaminów).

Komunikacja w trybie standardowym odbywa się wg poniższego diagramu:

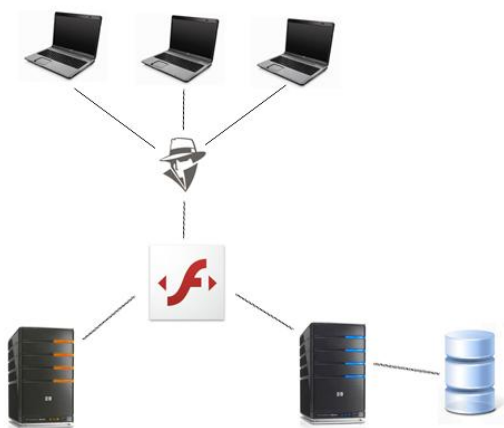


serwer i połączenia via http z trzema Klientami

W tym przypadku następuje poprzez protokół HTTP (http, amf). Powoduje to, że Klient bez większych trudnień widzi jakie informacje są przesyłane na serwer oraz jakie metody są w trakcie gry lub operacji wywoływane.

Koncepcją alternatywną jest wykorzystanie serwera **Flash Media Server** oraz szeregu zabezpieczeń, dzięki którym przechwytywanie informacji jest bardzo utrudnione, a wywoływanie funkcji zdalnych wymaga o wiele większego zaangażowania i wiedzy ze strony „pirata”.

Istotną kwestią jest usunięcie komunikacji w logice Klient-Serwer, co powoduje, iż zmienia się kompletnie metoda przesyłania informacji. Całość koncepcji opiera się o następujący diagram:



połączenie poprzez system weryfikacji oraz Flash Media Server z przesyłaniem informacji na serwery danych poprzez protokół RTMPE.

Istotną zmianą w komunikacji jest wykorzystanie serwera Flash Media Server z protokołem RTMPE, który jest enkodowany i zabezpieczony. W trakcie przesyłu następuje szereg weryfikacji – takich jak kontrolna „referrer url”, weryfikacji zgodności plików SWF, oraz nadawanie zwrotnych identyfikatorów. Te zabezpieczenia, choć są do obejścia ograniczają znacząco grupę amatorów chętnych do oszustwa.

Kolejnym zabezpieczeniem jest matryca wyników aktualizowana dynamicznie (w postaci np. wielowymiarowej tablicy), gdzie wyniki przesyłane są losowo (zakładamy nominalnie 2.500 komórek z rezultatem gry lub operacji).

Następnym zabezpieczeniem jest zapis gry w czasie rzeczywistym (zapis pozycji myszki, pozycji gracza, elementów kluczowych) oraz zapisywane w bazie danych wyniki z dowolnym interwałem (np. 3, 5 lub 15 sekund). Kolejną ewentualnością jest zapis „screenshot'ow” gry lub innej operacji na dysk serwera FMS.

Całość zabezpieczeń powoduje iż w naszej ocenie zmniejszamy ilość potencjalnych ataków o około 80%, a pozostałe 20% jesteśmy w stanie weryfikować za pomocą prostych narzędzi. Nie zdobędziemy się rzecz jasna na deklarację, iż 100% jest absolutnie osiągalne, jednakże zawęży to znacznie gardło, którym staje się bariera techniczna i konieczność operacji np. na niskim poziomie asemblera lub operacji na pamięci dynamicznej (chociażby narzędziu gameCheater). Dostępne jest także nagrywanie obrazu gry lub przebiegu egzaminu, co pozwala na „podglądanie” całości prowadzonych działań na ekranie Klienta.

Podsumowanie

Zapraszamy serdecznie do spotkania, na którym przedstawimy szerzej nasze rozwiązanie oraz możliwe formy współpracy.

Kontakt

Katashi / Ad-Ministry

05-825 Grodzisk Mazowiecki, Rusatki 2 / 22

NIP: 529-148-01-53

Regon: 014996922

www.katashi.pl

biuro@katashi.pl, biuro@ad-ministry.com