

Kraków - 10 czerwca - spotkanie OWASP i ISSA

<http://ipsec.pl/konferencje/2010/krakow-10-czerwca-spotkanie-owasp-issa.html>

Już w przyszły czwartek (10 czerwca 2010) ponownie spotykamy się na AGH. Tak jak poprzednio, spotkanie jest zorganizowane wspólnie z ISSA Polska.

Data i miejsce spotkania: 10 czerwiec 2010 Wydział Fizyki i Informatyki Stosowanej AGH ul. Reymonta 19, budynek D-10 Sala: A (aula) godz. 18:00-20:00

Agenda: 6:00pm - 6:15pm ... "OWASP News" - Przemysław Skowron 6:15pm - 7:10pm ... "Creating, obfuscating and analysis of JavaScript-based malware." - Krzysztof Kotowicz 7:15pm - 8:00pm ... "Network Forensic: what captured packets say" - Paweł Goleń

Wiecej informacji o prelekcjach:

1) Temat: "Tworzenie, zaciemnianie i analiza złośliwego kodu JavaScript"

Prelegent - Krzysztof Kotowicz: Web developer, specjalizuje się w tworzeniu rozwiązań e-commerce oraz portali internetowych z wykorzystaniem PHP 5. Freelancer, pracuje także w polskim portalu medycznym Medycyna Praktyczna. Jego głównym obszarem zainteresowań są zagadnienia bezpieczeństwa aplikacji internetowych oraz usprawnienia procesu tworzenia oprogramowania.

Abstrakt: Ataki malware'u na przeglądarki nieświadomych internautów stają się coraz powszechniejsze. Wciąż powstają nowe techniki pozwalające obejść filtry stosowane przez producentów oprogramowania zabezpieczającego. Z kolei filtry są coraz lepsze, powstają też nowe narzędzia - walka trwa. Na prezentacji dowiedziecie się, jak włamywacze usiłują utrudnić prace analizatorom ich kodu i jak reverserzy sobie z tym radzą. Nacisk zostanie położony na słabości narzędzi automatycznych - będziemy usiłowali uniknąć wykrycia przez jsunpack i Capture-HPC, oszukamy też popularny unpacker Deana Edwardsa.

2) Temat: "Network Forensic: co mówią schwyte pakiety"

Prelegent - Paweł Goleń: Obecnie pentester zajmujący się głównie testowaniem aplikacji internetowych. W międzyczasie dla rozrywki zajmuje się (nie tak bardzo) innymi tematami jak analiza malware czy network oraz computer forensic.

Abstrakt: Na poprzednim spotkaniu OWASP rozmawialiśmy o malware, między innymi o atakach "drive-by downloads". Tym razem kontynuacja tematu, prezentacja pokazuje co o tego typu incydentach można dowiedzieć się z zapisanego ruchu sieciowego. Jak na jego podstawie odtworzyć przebieg zdarzeń?

<https://lists.owasp.org/pipermail/owasp-poland/2010-June/000107.html>