

Ochrona danych i kryptografia

Praktyka i teoria

mgr inż. Maciej Miłostan

Politechnika Poznańska, Instytut Informatyki
Poznań, Polska

Konsultacje i kontakt

- Konsultacje: godziny konsultacji zostaną podane w późniejszym terminie
- E-mail: Maciej.Milostan@cs.put.poznan.pl
- Telefon: (+4861)6652826
- Pokój: 414 (ul. Piotrowo 3a)

Statystyka i sprawy organizacyjne

- Kto zetknął się w toku studiów z przedmiotem dotyczącym kryptografii lub ochrony danych?

Statystyka i sprawy organizacyjne

- Kto zetknął się w toku studiów z przedmiotem dotyczącym kryptografii lub ochrony danych?
- Kto nigdy nie zetknął się z tą tematyką?

Statystyka i sprawy organizacyjne

- Kto zetknął się w toku studiów z przedmiotem dotyczącym kryptografii lub ochrony danych?
- Kto nigdy nie zetknął się z tą tematyką?
- Kto zajmuje się tą tematyką zawodowo?

Statystyka i sprawy organizacyjne

- Kto zetknął się w toku studiów z przedmiotem dotyczącym kryptografii lub ochrony danych?
- Kto nigdy nie zetknął się z tą tematyką?
- Kto zajmuje się tą tematyką zawodowo?
- Proszę o przygotowanie listy z adresami e-mail.

Plan przedmiotu i sposob oceny

- Wykłady (8) i laboratoria (8)

Plan przedmiotu i sposob oceny

- Wykłady (8) i laboratoria (8)
- Na laboratoriach obecność obowiązkowa (można opuścić max. 2)

Plan przedmiotu i sposob oceny

- Wykłady (8) i laboratoria (8)
- Na laboratoriach obecność obowiązkowa (można opuścić max. 2)
- Zaliczenie na podstawie pisemnych sprawdzianów (testów) z wykładów i z laboratoriów.

Tematyka wykładów

- Patologia wirusów komputerowych, czyli jak się bronic przed wirusami. Przegląd programów antywirusowych.

Tematyka wykładów

- Patologia wirusów komputerowych, czyli jak się bronic przed wirusami. Przegląd programów antywirusowych.
- Incydenty w sieci i ochrona w sieci.

Tematyka wykładów

- Patologia wirusów komputerowych, czyli jak się bronic przed wirusami. Przegląd programów antywirusowych.
- Incydenty w sieci i ochrona w sieci.
- Fizyczna ochrona danych - archiwizacja, zapasowe centra danych, sieci SAN (Storage Area Networks).

Tematyka wykładów cd.

- Kryptografia - algorytmy kryptograficzne i ich implementacja, praktyczne zastosowanie kryptografii, elementy kryptoanalizy.

Tematyka wykładów cd.

- Kryptografia - algorytmy kryptograficzne i ich implementacja, praktyczne zastosowanie kryptografii, elementy kryptoanalizy.
- Steganografia - sztuka ukrywania informacji

Patologia wirusów - jak się bronić?

- Metody infekcji

Patologia wirusów - jak się bronić?

- Metody infekcji
 - proste skrypty w VBS,

Patologia wirusów - jak się bronić?

- Metody infekcji
 - proste skrypty w VBS,
 - przykłady programów w asemblerze i pascalu,

Patologia wirusów - jak się bronić?

- Metody infekcji
 - proste skrypty w VBS,
 - przykłady programów w asemblerze i pascalu,
 - przegląd błędów, używanych przez wirusy (np. msblaster), w systemach Windows.

Patologia wirusów - jak się bronić?

- Metody infekcji
 - proste skrypty w VBS,
 - przykłady programów w asemblerze i pascalu,
 - przegląd błędów, używanych przez wirusy (np. msblaster), w systemach Windows.
- Sposoby ochrony

Patologia wirusów - jak się bronić?

- Metody infekcji
 - proste skrypty w VBS,
 - przykłady programów w asemblerze i pascalu,
 - przegląd błędów, używanych przez wirusy (np. msblaster), w systemach Windows.
- Sposoby ochrony
 - przegląd programów antywirusowych,

Patologia wirusów - jak się bronić?

- Metody infekcji
 - proste skrypty w VBS,
 - przykłady programów w asemblerze i pascalu,
 - przegląd błędów, używanych przez wirusy (np. msblaster), w systemach Windows.
- Sposoby ochrony
 - przegląd programów antywirusowych,
 - wyłączanie zbędnych usług,

Patologia wirusów - jak się bronić?

- Metody infekcji
 - proste skrypty w VBS,
 - przykłady programów w asemblerze i pascalu,
 - przegląd błędów, używanych przez wirusy (np. msblaster), w systemach Windows.
- Sposoby ochrony
 - przegląd programów antywirusowych,
 - wyłączanie zbędnych usług,
 - aktualizacje.

Incydenty w sieci, zapobieganie...

- Klasyfikacja incydentów.

Incydenty w sieci, zapobieganie...

- Klasyfikacja incydentów.
- Monitorowanie sieci, narzędzia sieciowe, systemy IDS.

Incydenty w sieci, zapobieganie...

- Klasyfikacja incydentów.
- Monitorowanie sieci, narzędzia sieciowe, systemy IDS.
- Fałszowanie poczty, filtry antyspamowe.

Incydenty w sieci, zapobieganie...

- Klasyfikacja incydentów.
- Monitorowanie sieci, narzędzia sieciowe, systemy IDS.
- Fałszowanie poczty, filtry antyspamowe.
- Źródła informacji o błędach w zabezpieczeniach.

Fizyczna ochrona danych

- Świat po 11 września.

Fizyczna ochrona danych

- Świat po 11 września.
- Archiwizacja.

Fizyczna ochrona danych

- Świat po 11 września.
- Archiwizacja.
- Zapasowe centra danych.

Fizyczna ochrona danych

- Świat po 11 września.
- Archiwizacja.
- Zapasowe centra danych.
- Sieci SAN (Storage Area Networks).

Fizyczna ochrona danych

- Świat po 11 września.
- Archiwizacja.
- Zapasowe centra danych.
- Sieci SAN (Storage Area Networks).
- Łącza zapasowe.

Fizyczna ochrona danych

- Świat po 11 września.
- Archiwizacja.
- Zapasowe centra danych.
- Sieci SAN (Storage Area Networks).
- Łącza zapasowe.
- Podtrzymywanie zasilania - UPSy i generatory.

Kryptografia

- Algorytmy z kluczem tajnym (DES, Potrójny DES).

Kryptografia

- Algorytmy z kluczem tajnym (DES, Potrójny DES).
- Algorytmy z kluczem jawnym (RSA).

Kryptografia

- Algorytmy z kluczem tajnym (DES, Potrójny DES).
- Algorytmy z kluczem jawnym (RSA).
- Algorytmy wymiany kluczy (Diffiego-Helmana).

Kryptografia

- Algorytmy z kluczem tajnym (DES, Potrójny DES).
- Algorytmy z kluczem jawnym (RSA).
- Algorytmy wymiany kluczy (Diffiego-Helmana).
- Algorytmy haszowe (MD5, SHA).

Kryptografia

- Algorytmy z kluczem tajnym (DES, Potrójny DES).
- Algorytmy z kluczem jawnym (RSA).
- Algorytmy wymiany kluczy (Diffiego-Helmana).
- Algorytmy haszowe (MD5, SHA).
- System PGP i PEM.

Kryptografia

- Algorytmy z kluczem tajnym (DES, Potrójny DES).
- Algorytmy z kluczem jawnym (RSA).
- Algorytmy wymiany kluczy (Diffiego-Helmana).
- Algorytmy haszowe (MD5, SHA).
- System PGP i PEM.

Steganografia

Starożytna sztuka ukrywania informacji.



Figure 5. The Renoir cover file example (access <http://www.hs.port.ac.uk/wm/paint/auth/renoir/moulin-galette/>).



Figure 4. The satellite image we tested is of a major Soviet strategic bomber base (<http://edcwww.cr.usgs.gov/class/>).

+



Figure 9. The result of embedding the Airfield image in the Renoir cover with S-Tools.

Literatura