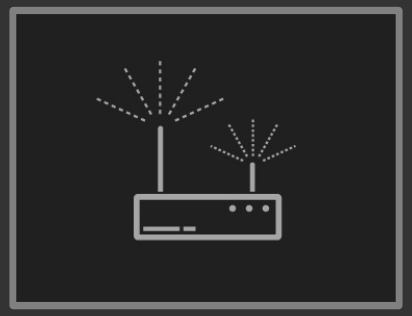
mindmade

WB Group

Jak shakować DRONa



Warszawa, marzec 2014

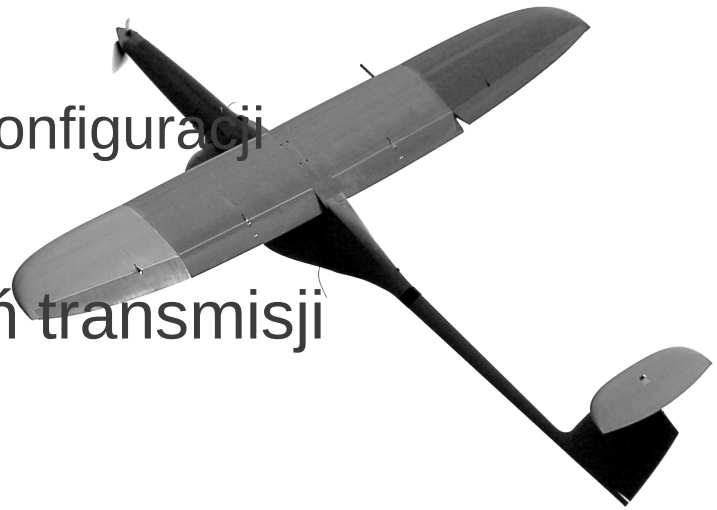
www.mindmade.pl

O nas

- Jesteśmy biurem projektowym
- Specjalizujemy się w
  - Kryptografii
  - Komunikacji
  - Systemach czasu rzeczywistego

Wyzwania – identyfikacja zagrożeń

- Bezzałogowe statki powietrzne narażone są na szereg zagrożeń związanych z przełamaniem zabezpieczeń:
  - Zmanipulowanie
  - Przejęcie (poprzez sterowanie)
  - Replikacja
  - Nieuprawniona zmiana misji, konfiguracji
  - Podszycie się
- Przełamamanie zabezpieczeń transmisji
  - Przejęcie informacji
  - Podmiana danych

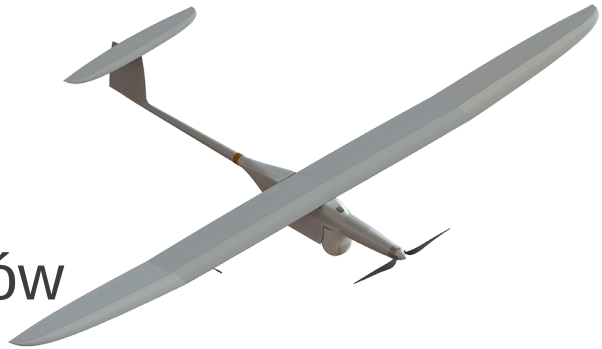


Chronione zasoby

- Oprogramowanie - często rozproszone na wiele bloków
- Dane
  - Konfiguracyjne
  - Identyfikacyjne
  - Zebrane
- Architektura oprogramowania – integralno
- Transmisja:
  - Poufność
  - Uwierzytelnienie stron połączenia

Podstawowe mechanizmy

- Szeroka paleta zabezpieczeń o charakterze kryptograficznym
  - Infrastruktura
  - Procedury
  - Odpowiednia siła mechanizmów
  - Roliczalność wykonywanych operacji
- Zabezpieczenia elektromechaniczne
  - Alarmy
  - Zdarzenia krytyczne niszczące i nieniszczące
- Zabezpieczenia mechaniczne



Kryptografia: o co chodzi?

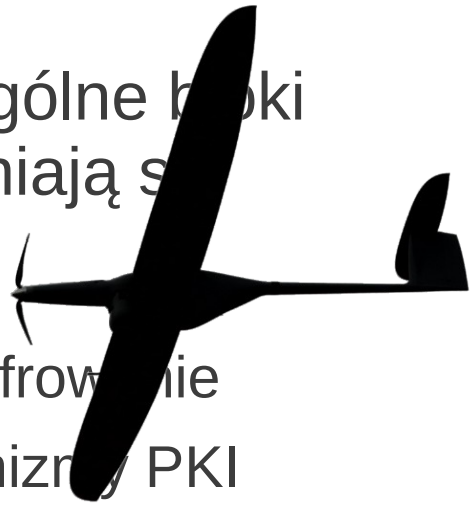
- … na pewno nie tylko o szyfrowanie!
- PKI
- Kryptograficzne mechanizmy zapewnienia integralności oraz autoryzacji zasobów
- Ustalanie kluczy szyfrujących
- … I wreszcie poufność danych oraz transmisji

Infrastruktura Klucza Publicznego

- Pozwala na
  - Uwierzytelnianie urządzeń I użytkowników
  - Przyjmowanie oraz wykluczanie (również zdalne) uczestników
  - Autoryzację praw
- PKI pozwala na kształtowanie polityki zabezpieczeń
- Mechanizmy PKI chronią system przed kompromitacją

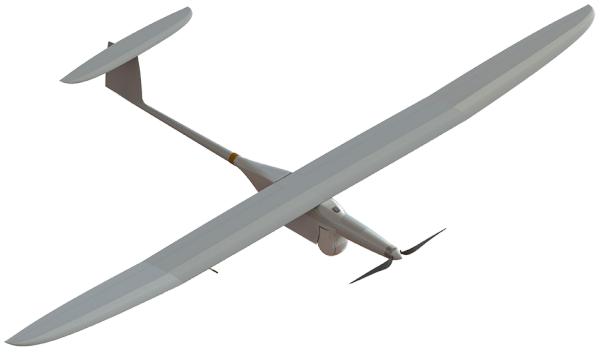
Ochrona zasobów

- Oprogramowanie: zaszyfrowane, chronione pod względem integralności
- Dane
  - Polityka zacierania danych ulotnych
  - Ochrona pod względem poufności oraz integralności danych nieulotnych
- Architektura oprogramowania: poszczególne bloki oprogramowania wzajemnie uwierzytelniają s
- Transmisja:
  - Poufność: ustalanie kluczy sesyjnych I szyfrowanie
  - Uwierzytelnienie stron połączenia: mechanizmy PKI



Zabezpieczenia elektromechaniczne

- Antypenetracyjne
- Integralność konstrukcji
- Współpraca mechaniki z oprogramowaniem



- Roliczalność: wielopoziomowy system logowania

Dziękuję za uwagę