

# Bezpieczeństwo systemów komputerowych

## Omijanie kryptografii

Marcin Peczarski

Instytut Informatyki Uniwersytetu Warszawskiego

4 listopada 2011

# Zarys problemu

- ▶ Nie wystarczy powiedzieć, że w naszej aplikacji stosujemy silną kryptografię.
- ▶ Kryptografię trzeba stosować umiejętnie.

# Architektura aplikacji

- ▶ Pewną aplikację zabezpieczono kluczem sprzętowym.
- ▶ Klucz sprzętowy używa silnej kryptografii, której złamanie jest nieopłacalne.
- ▶ Odtworzenie klucza wymaga:
  - ▶ zezlifowania zastosowanego układu scalonego i użycia mikroskopu elektronowego,
  - ▶ użycia wielu dni obliczeń superkomputera.
- ▶ Obsługa klucza sprzętowego zawarta jest w bibliotece łączonej dynamicznie (ang. *dll*), która nazywa się **DSWOVL** (bez rozszerzenia **DLL**, żeby było trudniej).
- ▶ Biblioteka ta zawiera tylko jedną funkcję **IOVLSLIB**, którą program główny wywołuje, chcąc sprawdzić obecność klucza.

# Atak

- ▶ Agresor:
  - ▶ przemianowuje bibliotekę `DSWOVL` na `DSWORG.DLL`.
  - ▶ tworzy własną wersję biblioteki `DSWOVL`.

# Zmienne globalne

```
FARPROC pfn1;  
HANDLE hOrgDll;
```

# Inicjowanie biblioteki dynamicznej

```
int WINAPI LibMain(HINSTANCE hInstance,
                  WORD wDataSeg,
                  WORD cbHeapSize,
                  LPSTR lpCmdLine) {
    hOrgDll = LoadLibrary("DSWORG.DLL");
    if ((int)hOrgDll >= 32) {
        pfn1 = GetProcAddress(hOrgDll,
                              MAKEINTRESOURCE(1));

        if (pfn1 == NULL) {
            MessageBox(0,
                      "Nie mogę wyznaczyć adresu "
                      "funkcji IOVLSLIB",
                      "LibMain",
                      0);
        }
    }
}
```

## Inicjowanie biblioteki dynamicznej, cd.

```
else { // hOrgDll < 32
    MessageBox(0,
               "Nie mogę załadować DSWORG.DLL",
               "LibMain",
               0);
}
return 1;
}
```

# Sprzątanie

```
int WINAPI WEP(int nParameter) {  
    if ((int)hOrgDll >= 32) {  
        FreeLibrary(hOrgDll);  
    }  
    return 1;  
}
```



# Główna funkcja

```
long _export WINAPI IOVLSLIB(char far* p1,  
                             char far* p2,  
                             char far* p3) {  
  
    long lResult;  
  
    if (pfn1) {  
        lResult = (*pfn1)(p1, p2, p3);  
        p1[57] = 1; // Klucz sprzętowy jest poprawny.  
    }  
    else {  
        lResult = 0;  
    }  
    return lResult;  
}
```

# Remedium

- ▶ Statyczna konsolidacja kodu obsługującego klucz sprzętowy.
- ▶ Zastosowanie rozwiązań utrudniających debugowanie.