

# Pluskwy, robale i inne paskudztwo

Aleksy Schubert  
Instytut Informatyki  
Uniwersytet Warszawski

20 listopada 2007

# Pluskwy

- Do informatyki wprowadzone przez tę

# Pluskwy

- Do informatyki wprowadzone przez tę



panią – admirał Grace Hooper

# Pluskwy

- Do informatyki wprowadzone przez tę



panią – admirał Grace Hooper

# Pluskwy

- Do informatyki wprowadzone przez Grace Hooper
- Pierwsza zachowana pluskwa wyglądała tak:

# Pluskwy

- Do informatyki wprowadzone przez Grace Hooper
- Pierwsza zachowana pluskwa wyglądała tak:

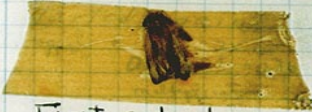
9/9

0800 Antan started  
1000 " stopped - antan ✓ { 1.2700 9.037 847 025  
13<sup>00</sup> MC (032) MP-MC 1.5826000 9.057 846 995 connect  
                  (033) PRO 2 2.130476415 (032) 4.615925059(-2)  
                  connect 2.130676415

Relays 6-2 in 033 failed special speed test  
in relay .. 10.00 test.

Relays changed

1100 Started Cosine Tape (Sine check)  
1525 Started Multi-Adder Test.

1545  Relay #70 Panel F  
(moth) in relay.

First actual case of bug being found.

1630 Antan started.  
1700 closed down.

Relay 3145  
Relay 3376

# Pluskwy

- Do informatyki wprowadzone przez Grace Hooper
- Pierwsza zachowana pluskwa to ćma znaleziona 9 września 1947 roku
- Termin ten był używany przez inżynierów jeszcze w XIX wieku

# Pluskwy

- ...
- Termin ten był używany przez inżynierów jeszcze w XIX wieku
- Pluskwy są niebezpieczne

# Pluskwy

- ...
- Termin ten był używany przez inżynierów jeszcze w XIX wieku
- Pluskwy są niebezpieczne



# Pluskwy

- Do informatyki wprowadzone przez Grace Hooper
- Pierwsza zachowana pluskwa to była ćma znaleziona 9 września 1947 roku
- Termin ten był używany przez inżynierów jeszcze w XIX wieku
- Pluskwy są niebezpieczne
- ...i bardzo trudne do wykrycia

# Pluskwy

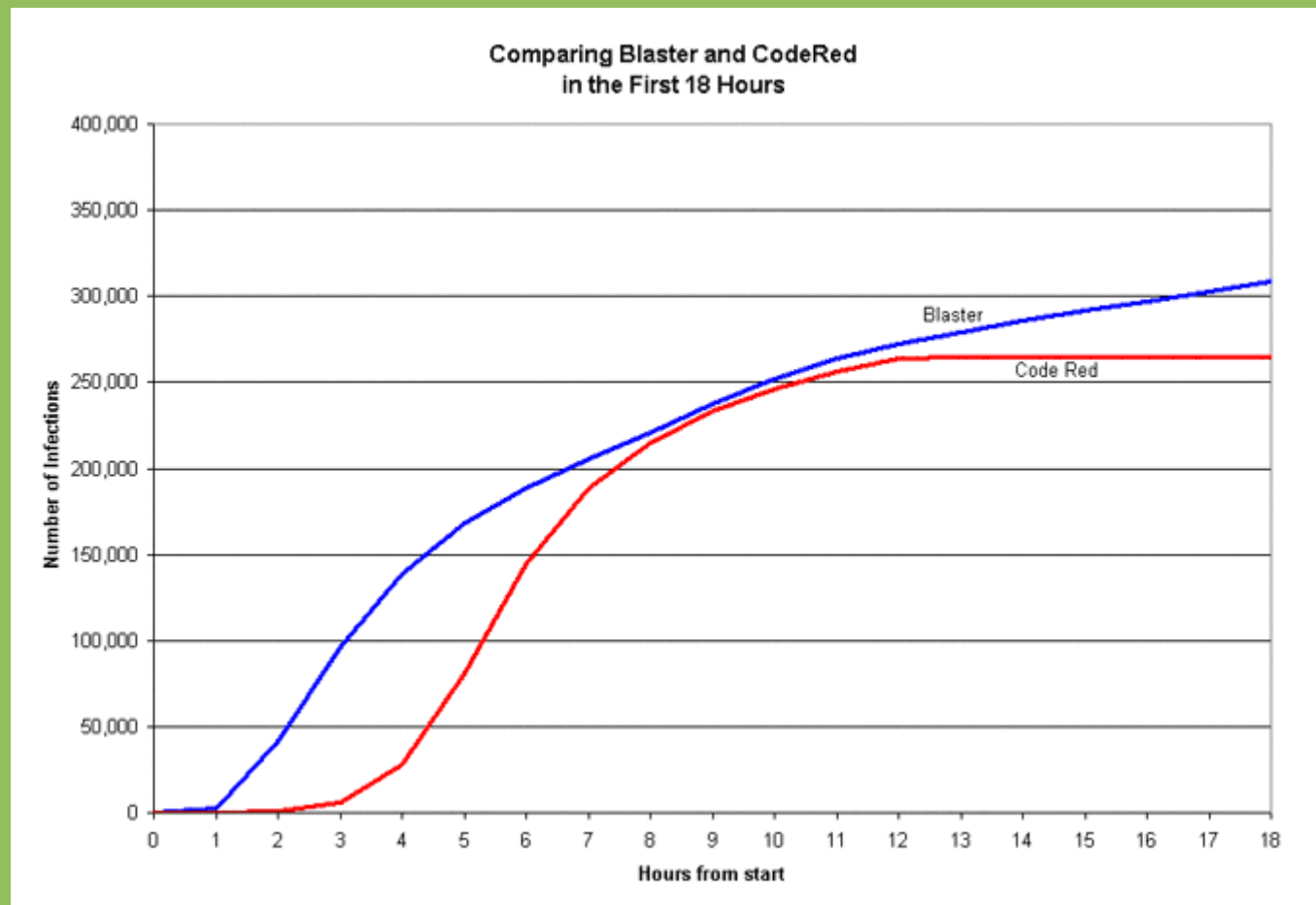
...tym bardziej,  
że nie wiadomo,  
czym są...

# Robale

- Pierwszy internetowy robal użyty był w laboratoriach Xerox-a w roku 1978
- Opis pojawił się w 1982 roku
- Pierwszy złośliwy robal powstał w roku 1989 napisany przez Roberta Morrisa
- Wykorzystywał kilka prostych luk:
  - sendmail, fingerd, rsh/rexec
- Tylko kopiowanie

# Robale

- Szybkość rozprzestrzeniania się:



# Robale

- Robert Morris stanął przed sądem
  - 3 lata okresu próbnego
  - 400 godzin prac publicznych
  - 10 050 dolarów grzywny

Były przypadki, że w wyniku działania robali unieruchomiony został sprzęt lekarski

# Inne paskudztwo

- Wirusy, makrowirusy
- Spam
- Konie trojańskie
- Adware
- Spyware
- ...

# Jak temu zaradzić?

- Wyszukiwarki błędów
- Piaskownice i wirtualizacja
- Skanery wirusów
- Zapory ogniowe
- Certyfikaty
- PCC (proof-carrying code)
- ...

# Wyszukiwarki błędów

- Pierwszy problem – czym jest błąd
- Podstawowy rodzaj błędu – *przekroczenie zakresu bufora*
- Trzeba używać funkcji `snprintf` zamiast `sprintf`
- Wady:
  - można przekroczenie zakresu uzyskać inaczej
  - wiele alarmów jest zbędne

# Piaskownice i wirtualizacja

- Program działa w obudówce (piaskownicy)
- Jeśli chce wykonać podejrzaną operację (np. skasowanie pliku) obudówka mu
  - zabrania albo
  - pyta się użytkownika, czy można
- *Wirtualizacja* – można zrobić obudówkę dla całego systemu operacyjnego

# Skannery wirusów

- Tworzenie i badanie sygnatur programów
- Wyłapywanie charakterystycznych wzorców
- Przypomina to trochę *core wars*
- Wady:
  - konieczność odświeżania oprogramowania antywirusowego
  - programy mogą ulec popsuciu w wyniku naprawy systemu

# Zapory ogniowe

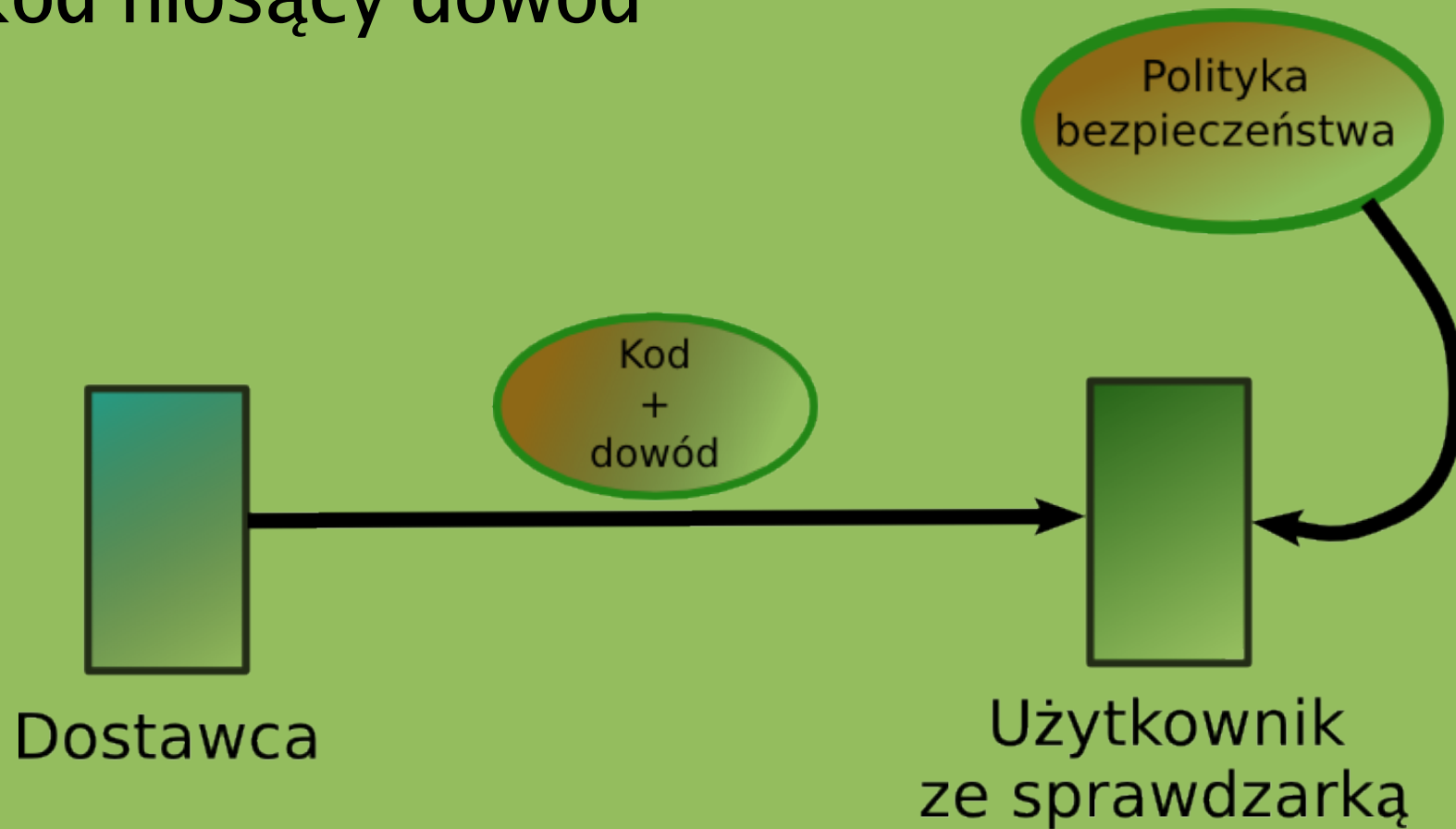
- Oddzielna sieć i maszyna odpowiedzialne za dostęp do Internetu
- Maszyna ma za zadanie:
  - ograniczać ruch
  - obsługiwać narażone usługi
- Wady:
  - potrzebna oddzielna maszyna
  - ograniczenia w funkcjonalności

# Certyfikaty

- Po części używane w programach antywirusowych
- Dystrybutor programu oblicza skrót (np. SHA1) programu i go podpisuje
- Określenie odpowiedzialności
- Wady:
  - problemy z budowaniem zaufania
  - problemy z uzyskaniem zaufania przez dystrybutorów

# Proof-carrying code

- Kod niosący dowód



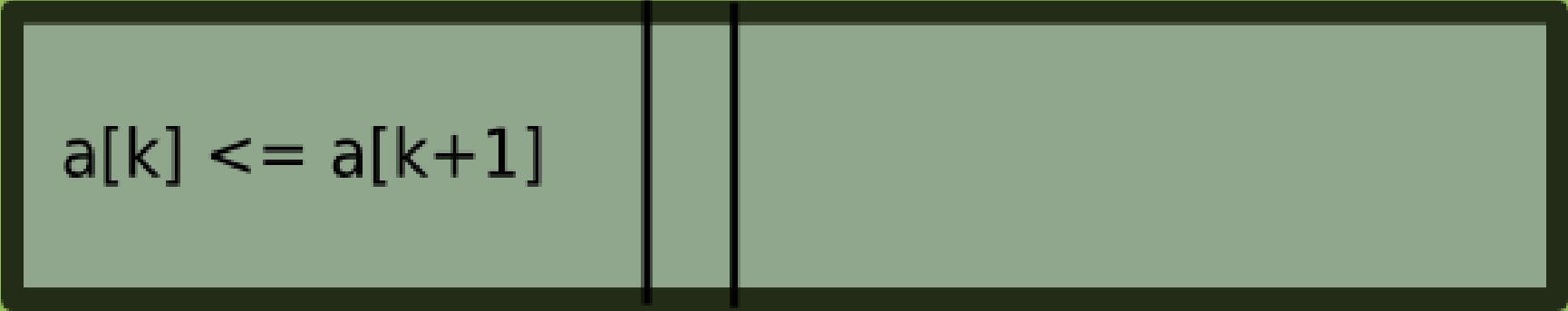
# Kod niosący dowód

- Proof-carrying code
- Matematyczna pewność poprawności
- Musi być wiadomo, czym jest błąd
- Wady:
  - pracochoćność
  - trudno uzyskać rzetelną sprawdzarkę

# Zadanie

```
int a[], int rozmiar;
int i, j, min;
i=0;
while (i < rozmiar) {
    min = i; j = i+1;
    while (j < rozmiar) {
        if (a[j] < a[min]) {
            min = j;
        }
        j = j+1;
    }
    zamien(i, min, a);
    i = i+1;
}
```

# Zadanie



The diagram shows a horizontal array represented by a light gray rectangle with a thick black border. Two vertical black lines divide the array into three sections. The leftmost section contains the text  $a[k] \leq a[k+1]$ . The middle section is narrow and empty. The rightmost section is the largest and is also empty. Below the array, the letter  $i$  is centered under the middle section.

$a[k] \leq a[k+1]$

$i$

# Zadanie

## Założenia:

- $a$  zawiera liczby naturalne, jej rozmiar jest liczbą naturalną
- `rozmiar` to liczba elementów  $a$
- `zamien(x, y, b)` zamienia miejscami elementy na pozycjach  $x, y$  w  $b$

# Zadanie

## Pytania:

- Czy przebieg wykonania jest bezbłędny?
- Czy elementy w  $a$  po wykonaniu operacji ustawione są rosnąco?
- Czy elementy w  $a$  po wykonaniu operacji są takie same jak przed wykonaniem?

**Miłej zabawy!**