
LIVE

co fascynuje mnie w hakingu

Gynvael Coldwind

MEGA Sekurak Hacking Party, Kraków, 2019

If you are reading these slides (i.e. not watching the actual talk)
please note there are speaker notes under each slide.

whoami

Tech Lead / Manager @ Google ISE-RIP

All opinions expressed during this presentation are mine and mine alone, and not those of my barber, my accountant or my employer.

Jadłospis

- Odpowiedź na pytanie.
- Wyjaśnienie poprzez przykłady.
  A tak w zasadzie to ukłon w stronę świetnych badaczy!
- Trochę losowych porad i odpowiedzi.

Full disclosure: Kilka slajdów pochodzi z innych moich prezentacji.

"Haking" i "hakerzy" - definicje

Jak zwykle, jest kilka definicji.

"Haking" i "hakerzy" - definicje

Hacker (n.)

> One who writes 'hacky' code.

(Definicja w zasadzie związana z programowaniem. Niemłoda, ale nadal używana.)

"Haking" i "hakerzy" - definicje
→ Chwila, co to jest "hack" w programowaniu?

Przykład: Wyraź 8-bitową liczbę w systemie binarnym

`3 → 00000011`

`42 → 00101010`

"Haking" i "hakerzy" - definicje
→ Chwila, co to jest "hack" w programowaniu?

Przykład: Wyraź 8-bitową liczbę w systemie binarnym

```
void to_bin(uint8_t n, char *output) {
  for (int i = 7; i >= 0; i--)
    if (((n >> i) & 1) == 1)
      output[7 - i] = '1';
    else
      output[7 - i] = '0';
}
```

Dla każdego bitu, wybierz ten jeden bit, po czym wypisz "1" or "0" w zależności od wartości owego bitu.

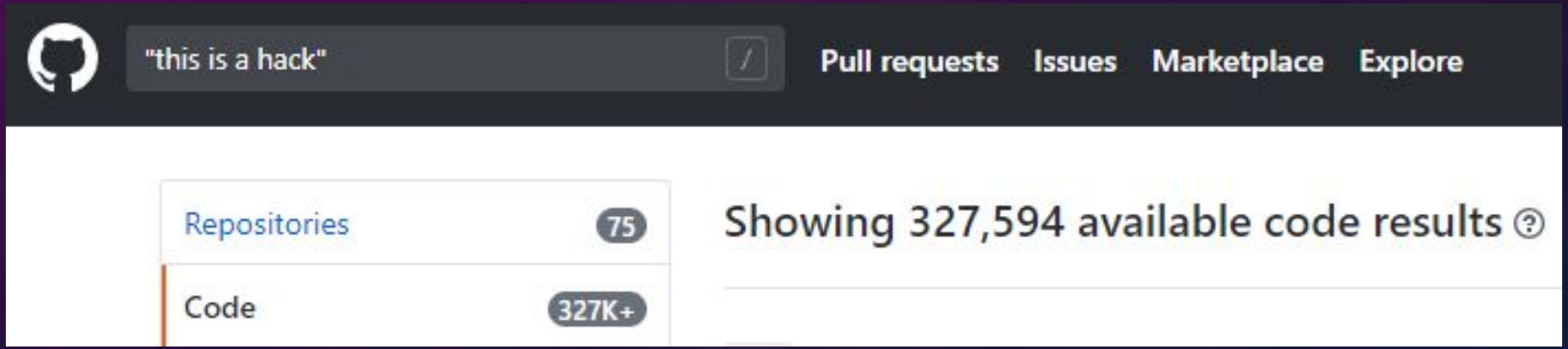
"Haking" i "hakerzy" - definicje
→ Chwila, co to jest "hack" w programowaniu?

Przykład: Wyraź 8-bitową liczbę w systemie binarnym

```
void to_bin_better(uint8_t n, char *output) {
 *(uint64_t*)output = 3472328296227680304ULL +
   (((n * 9241421688590303745ULL) / 128) &
   72340172838076673ULL);
}
```

Chwila... co?
Uhm, nie wiem?
Ten kod w ogóle działa?

"Haking" i "hakerzy" - definicje
→ Chwila, co to jest "hack" w programowaniu?



"Haking" i "hakerzy" - definicje

Hacker (n.)

> A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular.

Źródło: https://tools.ietf.org/html/rfc1392 - Internet Users' Glossary

Patrz również: https://en.wikipedia.org/wiki/Hacker_culture

A także: https://en.wikipedia.org/wiki/Hackerspace

"Haking" i "hakerzy" - definicje

Hacker (n.)

[1] A computer security professional.

[2] [...] someone who seeks to breach defenses and exploit weaknesses in a computer system or network

Źródła:

[1] https://en.wiktionary.org/wiki/hacker

[2] https://en.wikipedia.org/wiki/Security_hacker

"Haking" i "hakerzy" - definicje

Nieprawidłowa, ale dość popularna potocznie definicja (Patrz również: *teoria*)

Hacker (n.)

Osoba, która nielegalnie włamuje się do sieci lub systemów komputerowych w złośliwych celach.

Patrz również:

https://en.wikipedia.org/wiki/Hacker#Representation_of_Hackers_in_Mainstream_Media

"Haking" i "hakerzy" - definicje

Przykład zamieszania
(znalezione na Wikipedii)

"Some members of this breed of hacker eventually go corporate. For example, Linus Torvalds, the man who wrote the central component for the Linux operating system, has a well-respected hacking history."

"A who's who of hackers" Fortune Magazine

Patrz również:

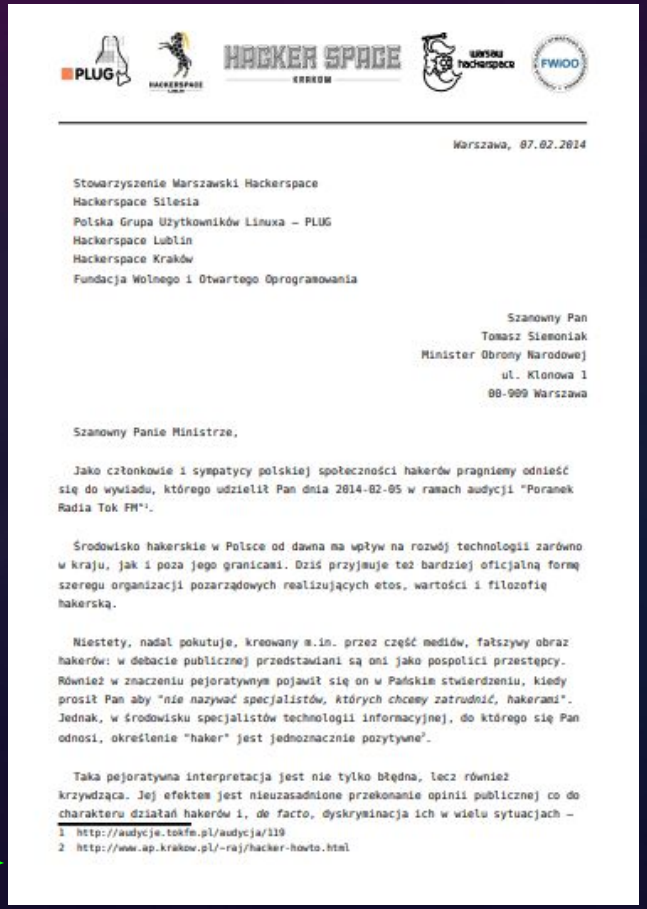
https://en.wikipedia.org/wiki/Hacker#Representation_of_Hackers_in_Mainstream_Media

"Haking" i "hakerzy" - definicje

"Nie powiedziałbym, że zatrudniamy hakerów, tylko zatrudniamy świetnych specjalistów. Proszę ich nie nazywać hakerami."

Minister Obrony Narodowej
w wywiadzie dla TOK FM

Odpowiedź od środowisk hakerskich w postaci otwartego listu



Warszawa, 07.02.2014

Stowarzyszenie Warszawski Hackerspace
Hackerspace Silesia
Polska Grupa Użytkowników Linuxa – PLUG
Hackerspace Lublin
Hackerspace Kraków
Fundacja Wolnego i Otwartego Oprogramowania

Szanowny Pan
Tomasz Siemoniak
Minister Obrony Narodowej
ul. Klonowa 1
00-909 Warszawa

Szanowny Panie Ministrze,

Jako członkowie i sympatycy polskiej społeczności hakerów pragniemy odnieść się do wywiadu, którego udzielił Pan dnia 2014-02-05 w ramach audycji "Poranek Radia Tok FM"[1].

Środowisko hakerskie w Polsce od dawna ma wpływ na rozwój technologii zarówno w kraju, jak i poza jego granicami. Dziś przyjmuje też bardziej oficjalną formę szeregu organizacji pozarządowych realizujących etos, wartości i filozofię hakerską.

Niestety, nadal pokutuje, kreowany m.in. przez część mediów, fałszywy obraz hakerów: w debacie publicznej przedstawiani są oni jako pospolici przestępcy. Również w znaczeniu pejoratywnym pojawił się on w Pańskim stwierdzeniu, kiedy prosił Pan aby *"nie nazywać specjalistów, których chcemy zatrudnić, hakerami"*. Jednak, w środowisku specjalistów technologii informacyjnej, do którego się Pan odnosi, określenie "haker" jest jednoznacznie pozytywne[2].

Taka pejoratywna interpretacja jest nie tylko błędna, lecz również krzywdząca. Jej efektem jest nieuzasadnione przekonanie opinii publicznej co do charakteru działań hakerów i, *de facto*, dyskryminacja ich w wielu sytuacjach –

1 http://audycje.tokfm.pl/audycja/119
2 http://www.ap.krakow.pl/~raj/hacker-howto.html

"Haking" i "hakerzy" - definicje

Hacker (n.)

(US) One who operates a taxicab

Źródło: https://en.wiktionary.org/wiki/hacker#English

"Haking" i "hakerzy" - definicje

Proszę założyć, że podczas tej prelekcji mówiąc "haker" lub "haking" mam na myśli:

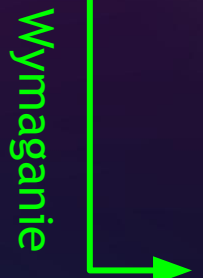
"Haking" i "hakerzy" - definicje

Proszę założyć, że podczas tej prelekcji mówiąc "haker" lub "haking" mam na myśli:

A CAB DRIVER

"Haking" i "hakerzy" - definicje

Proszę założyć, że podczas tej prelekcji mówiąc "haker" lub "haking" mam na myśli:



A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular.

A computer security professional.
[...] someone who seeks to breach defenses and exploit weaknesses in a computer system or network

Więc, co mnie trzyma przy hakingu?

Szczegóły

małe kawałki informacji

najczęściej zwykłe ciekawostki bez większego znaczenia

Więc, co mnie trzyma przy hakingu?

Szczegóły

małe kawałki informacji

najczęściej zwykłe ciekawostki bez większego znaczenia

a przynajmniej dopóki nie wpadną na swoje miejsce jak ostatni kawałek układanki

Więc, co mnie trzyma przy hakingu?

Szczegóły

małe kawałki informacji

najczęściej zwykłe ciekawostki bez większego znaczenia

a przynajmniej dopóki nie wpadną na swoje miejsce jak ostatni kawałek układanki

To one sprawiają, że haking jest taki ciekawy.
Z czasem, zaczyna się je kolekcjonować.

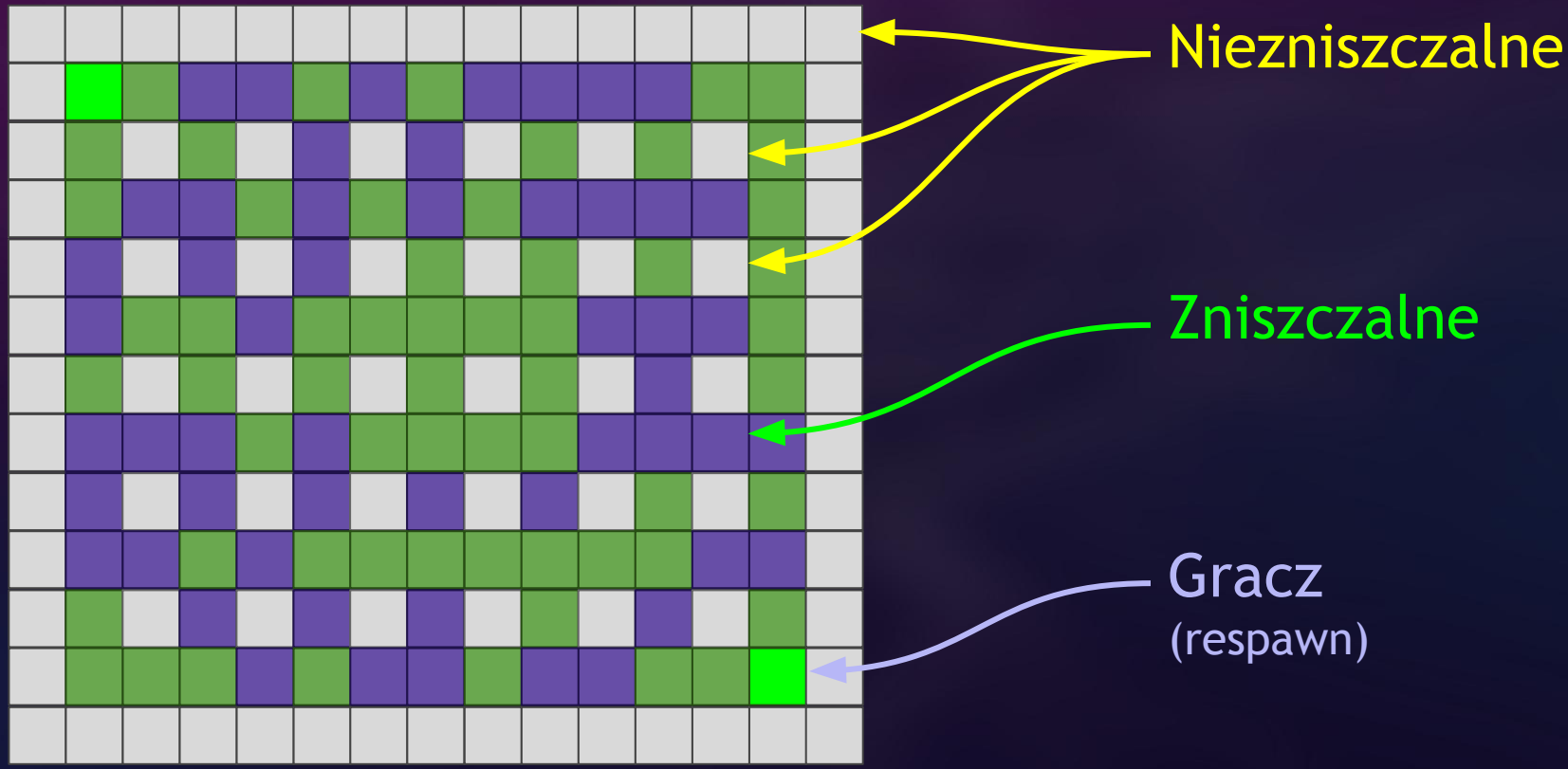
Zacznijmy prosto

Szczegóły na przykładach #1

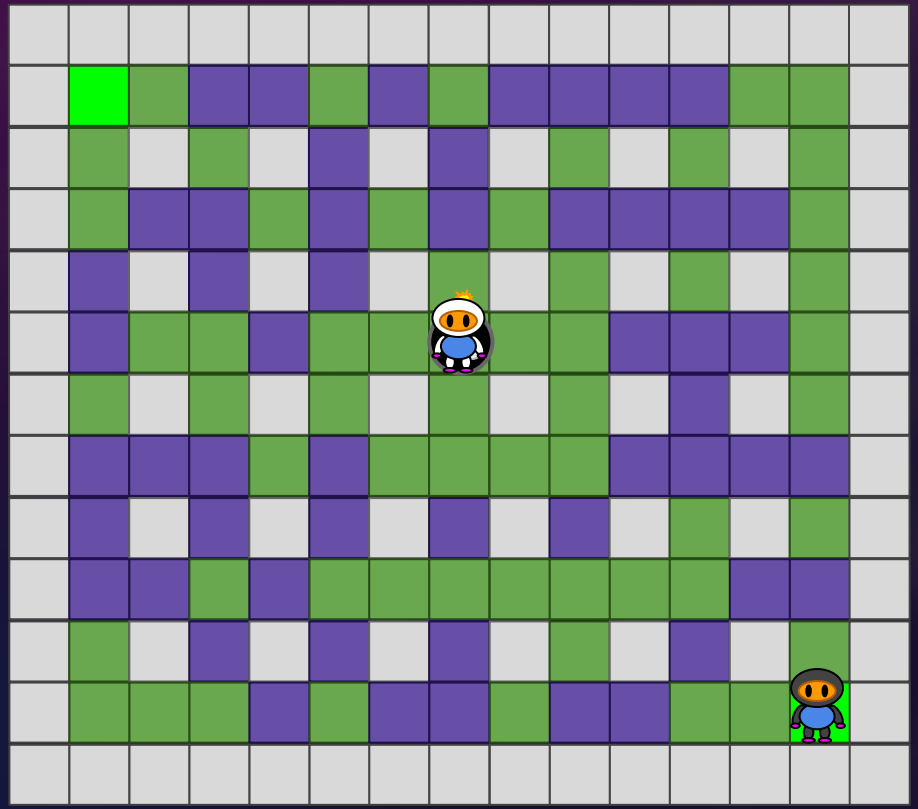
Dyna Blaster / Bomberman (Hudson Soft, 1991)

Na czym ta gra polega?

Na czym ta gra polega?

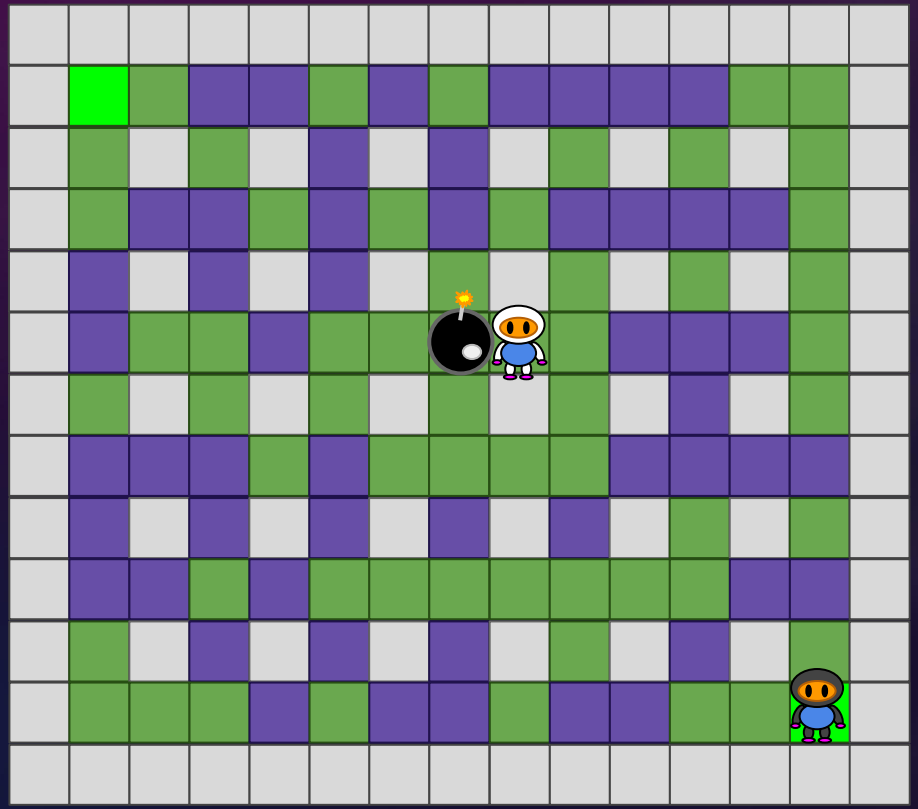


Na czym ta gra polega?



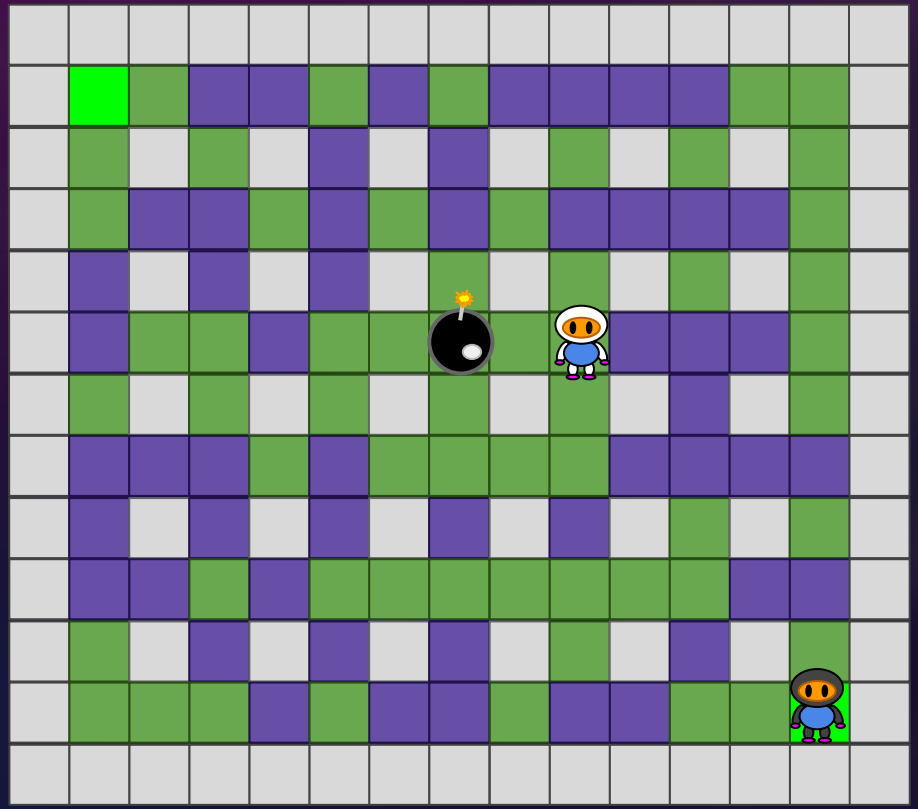
Gracz może podłożyć bombę na swojej pozycji.

Na czym ta gra polega?



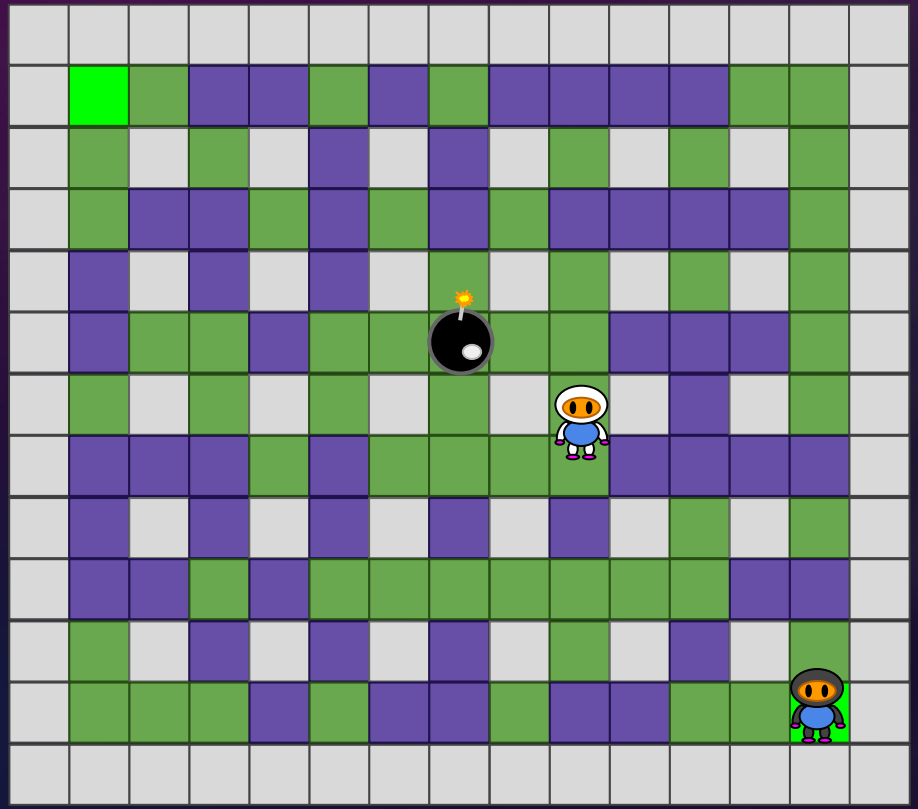
Gracz może podłożyć bombę na swojej pozycji.

Na czym ta gra polega?



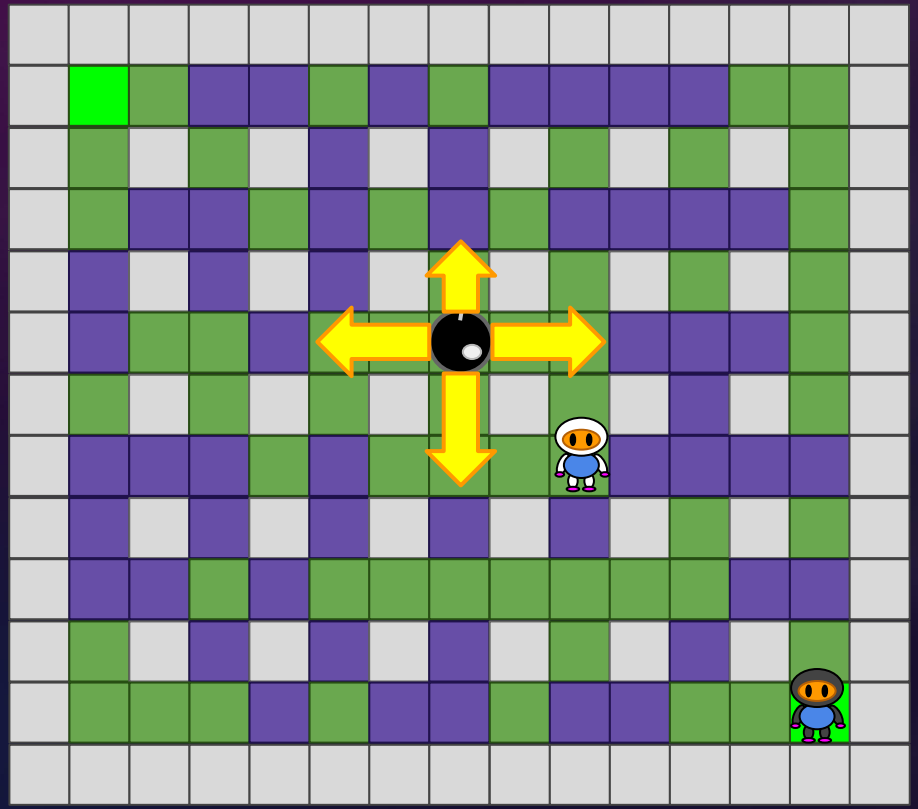
Gracz może podłożyć bombę na swojej pozycji.

Na czym ta gra polega?



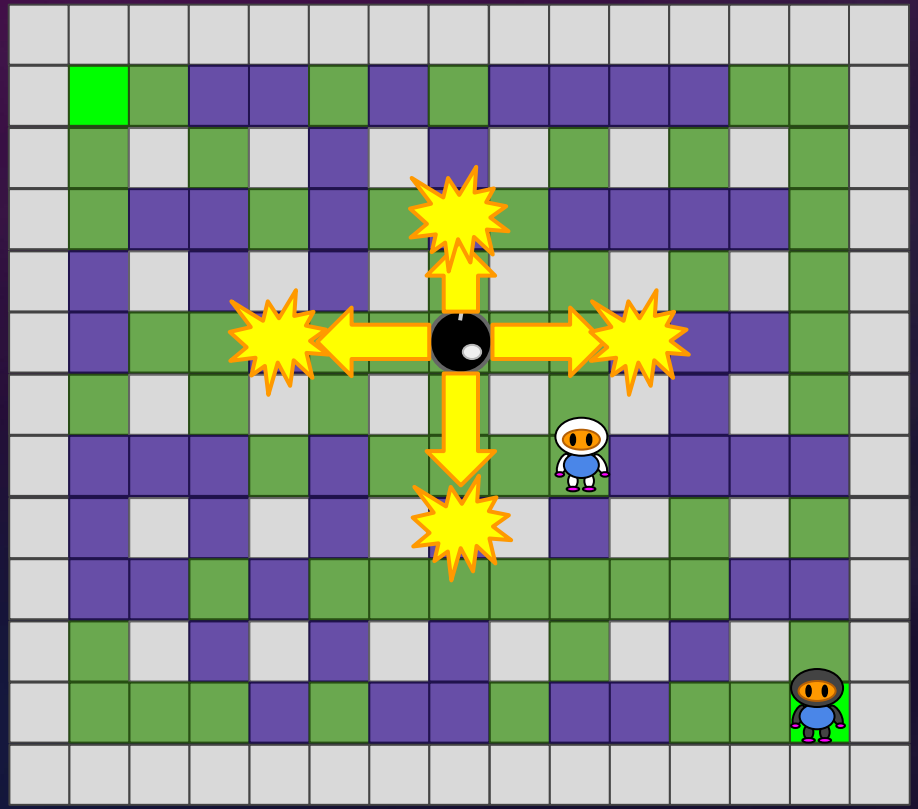
Gracz może podłożyć bombę na swojej pozycji.

Na czym ta gra polega?



Bomba wybucha po około 3 sekundach (pionowo i poziomo).

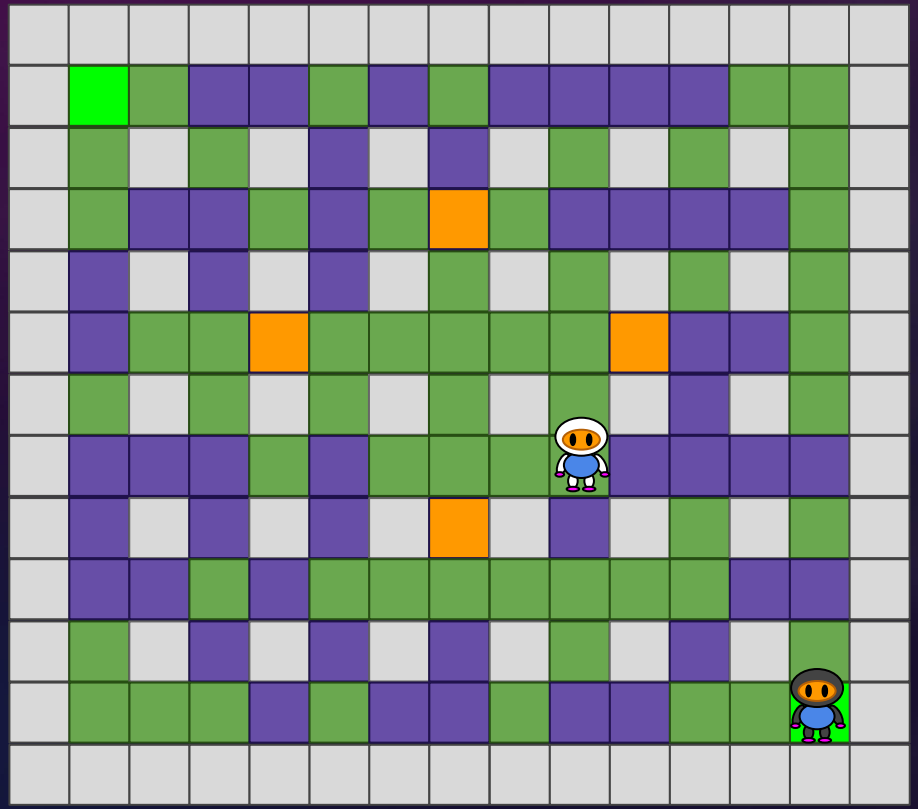
Na czym ta gra polega?



Bomba wybucha po około 3 sekundach (pionowo i poziomo).

I niszczy pierwsze napotkane ściany w swoim zasięgu.

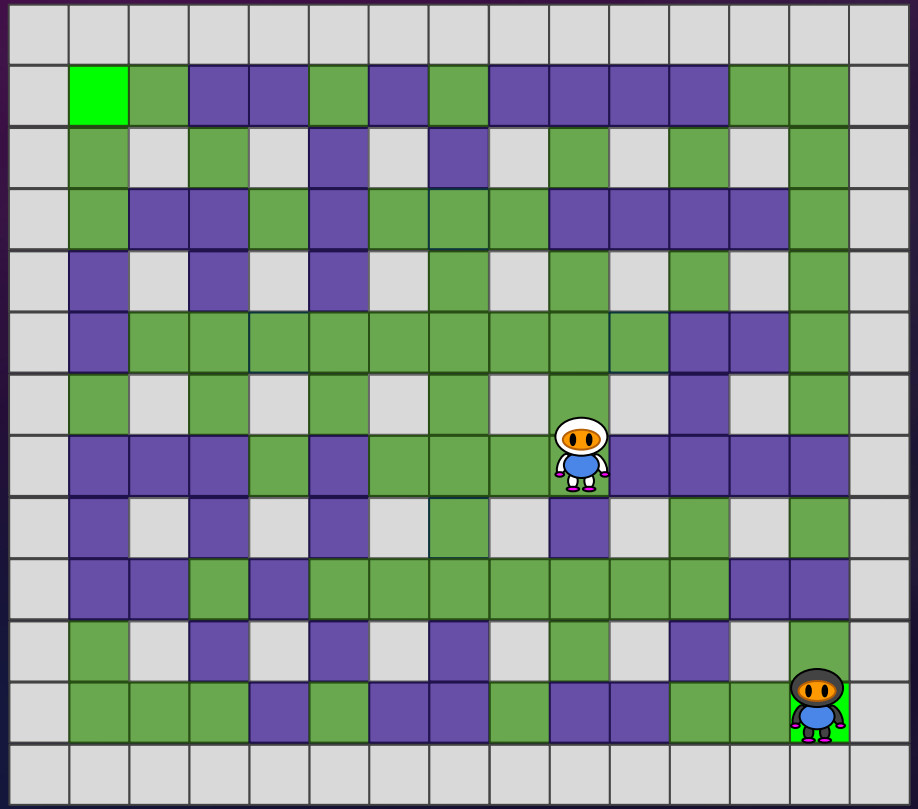
Na czym ta gra polega?



Bomba wybucha po około 3 sekundach (pionowo i poziomo).

I niszczy pierwsze napotkane ściany w swoim zasięgu.

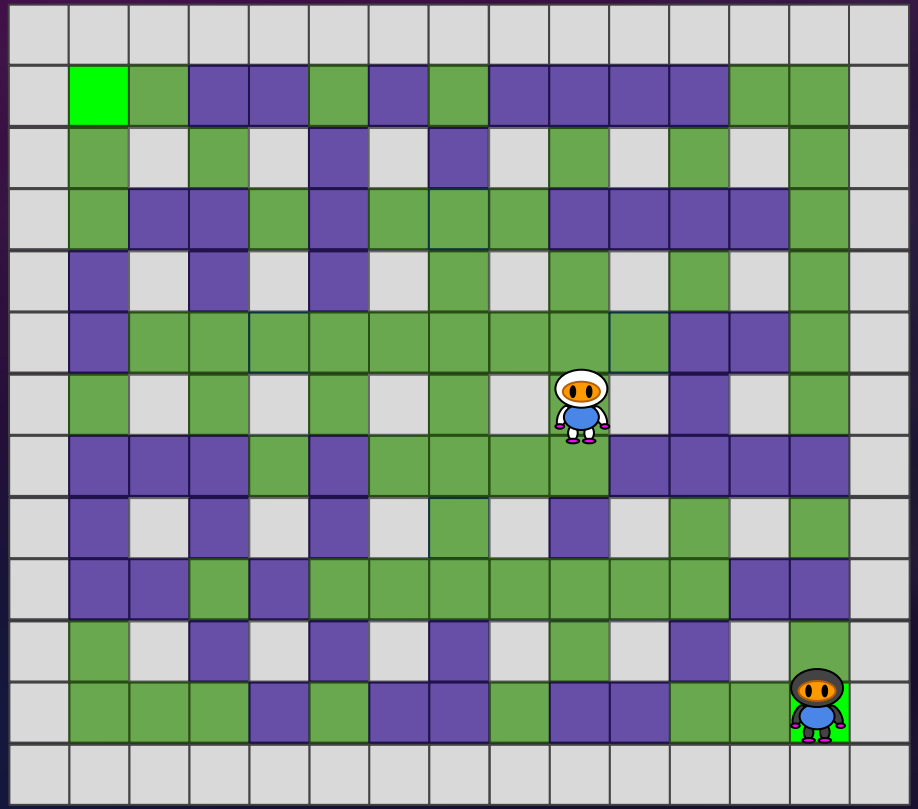
Na czym ta gra polega?



Bomba wybucha po około 3 sekundach (pionowo i poziomo).

I niszczy pierwsze napotkane ściany w swoim zasięgu.

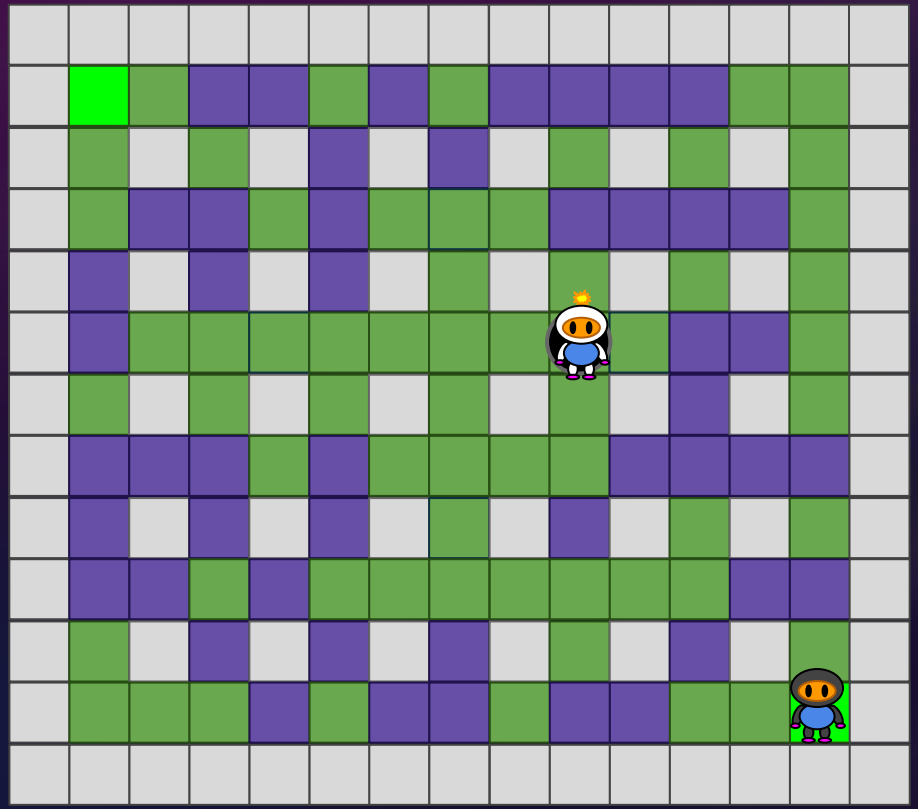
Na czym ta gra polega?



Gracz nie mogą przechodzić przez bomby.

(Wyjątek: można "zejść" z bomby po jej podłożeniu)

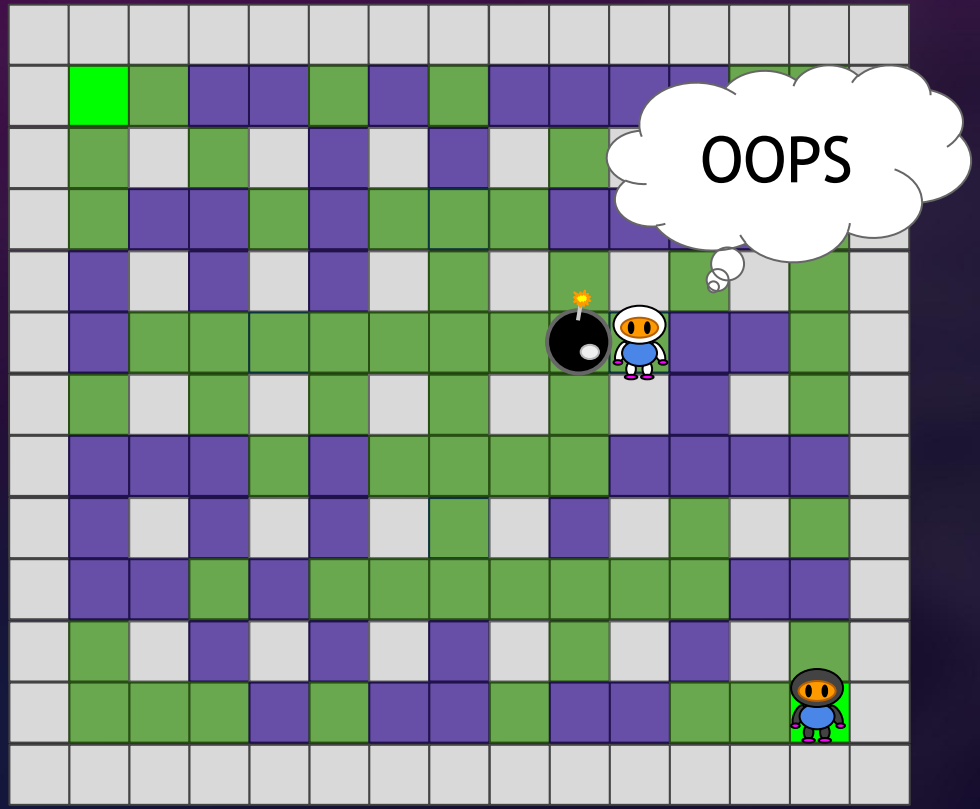
Na czym ta gra polega?



Gracz nie mogą przechodzić przez bomby.

(Wyjątek: można "zejść" z bomby po jej podłożeniu)

Na czym ta gra polega?

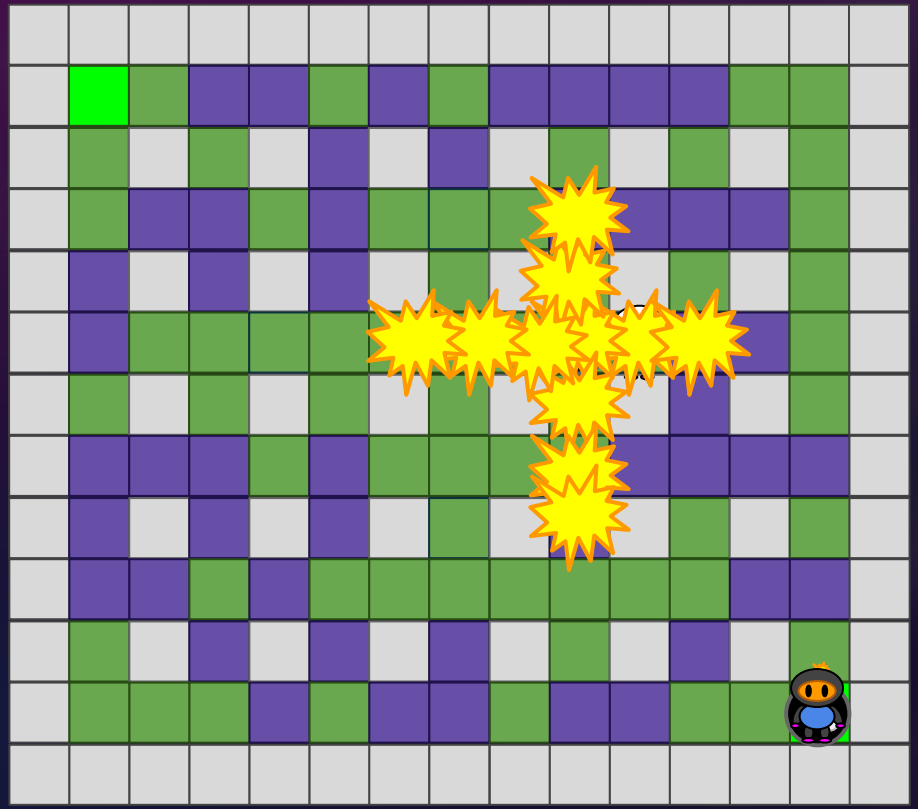


Gracz nie mogą przechodzić przez bomby.

(Wyjątek: można "zejść" z bomby po jej podłożeniu)

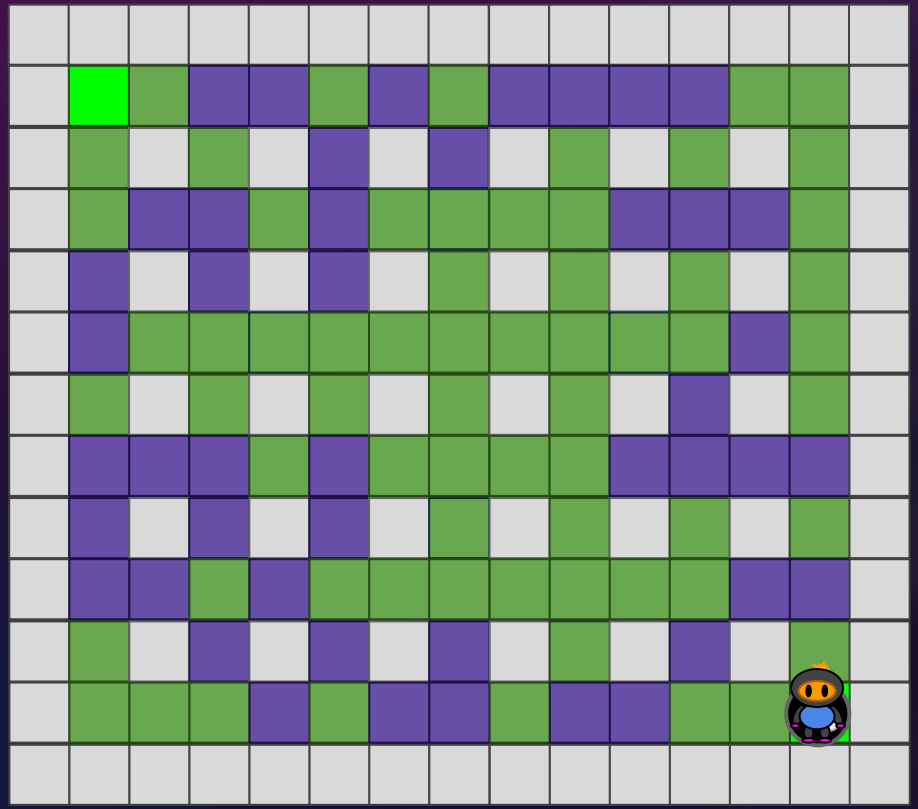
(Tak większość graczy przegrywa)

Kryteria wygranej?



Wygrywa ostatni gracz pozostający na planszy!

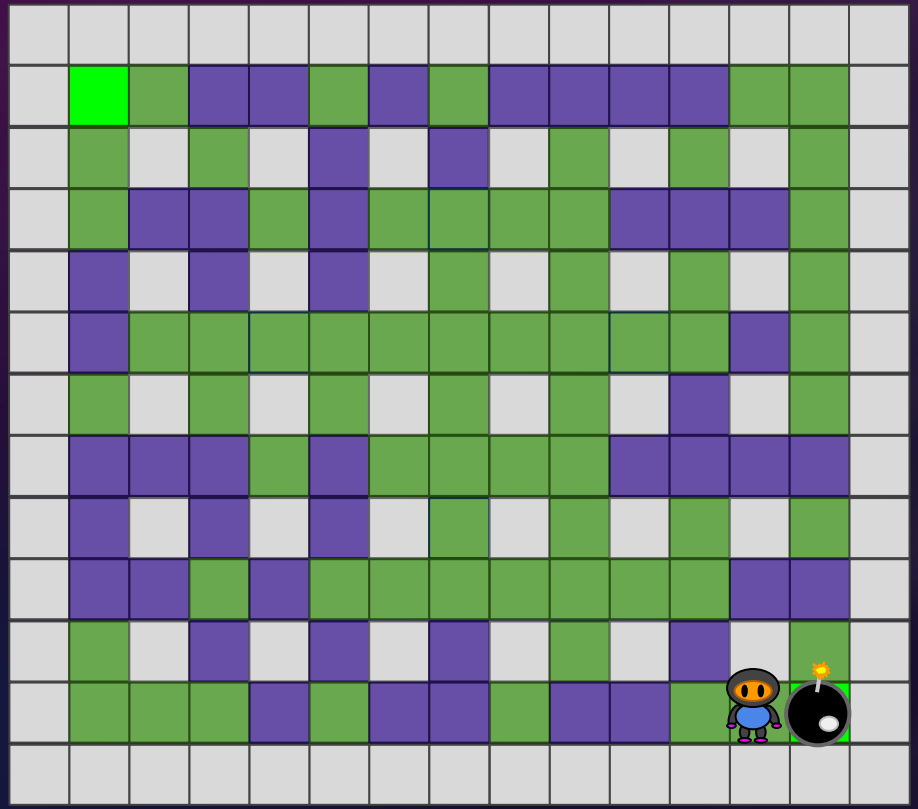
Kryteria wygranej?



Wygrywa ostatni gracz pozostający na planszy!

Ale musi jeszcze przeżyć 5 sekund (tak, żeby wszystkie bomby eksplodowały).

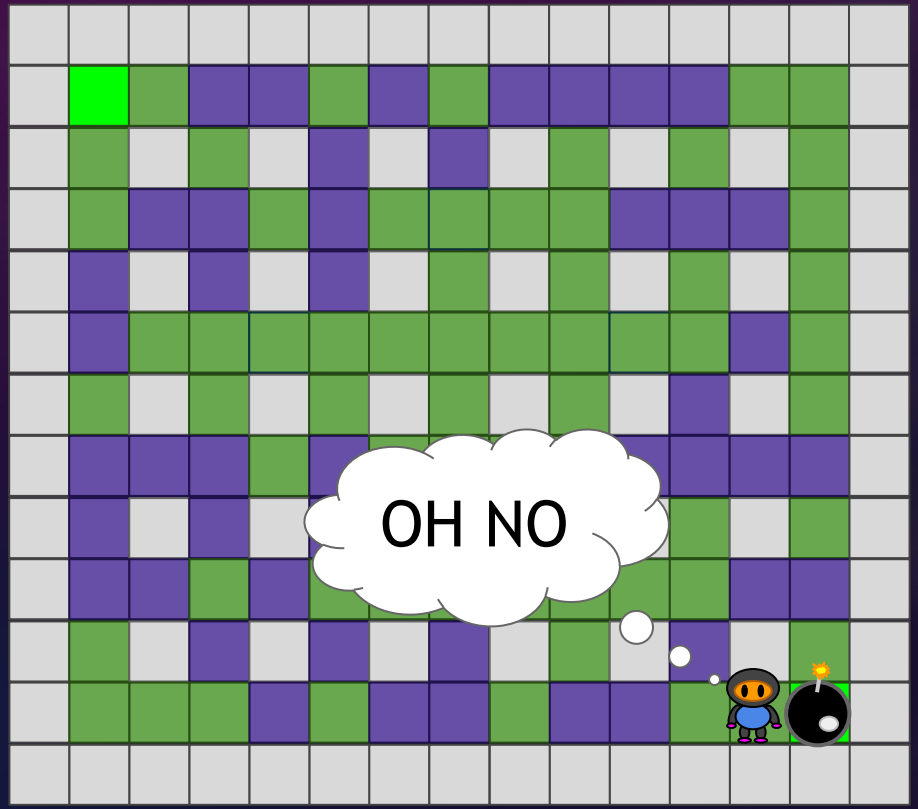
Kryteria wygranej?



Wygrywa ostatni gracz pozostający na planszy!

Ale musi jeszcze przeżyć 5 sekund (tak, żeby wszystkie bomby eksplodowały).

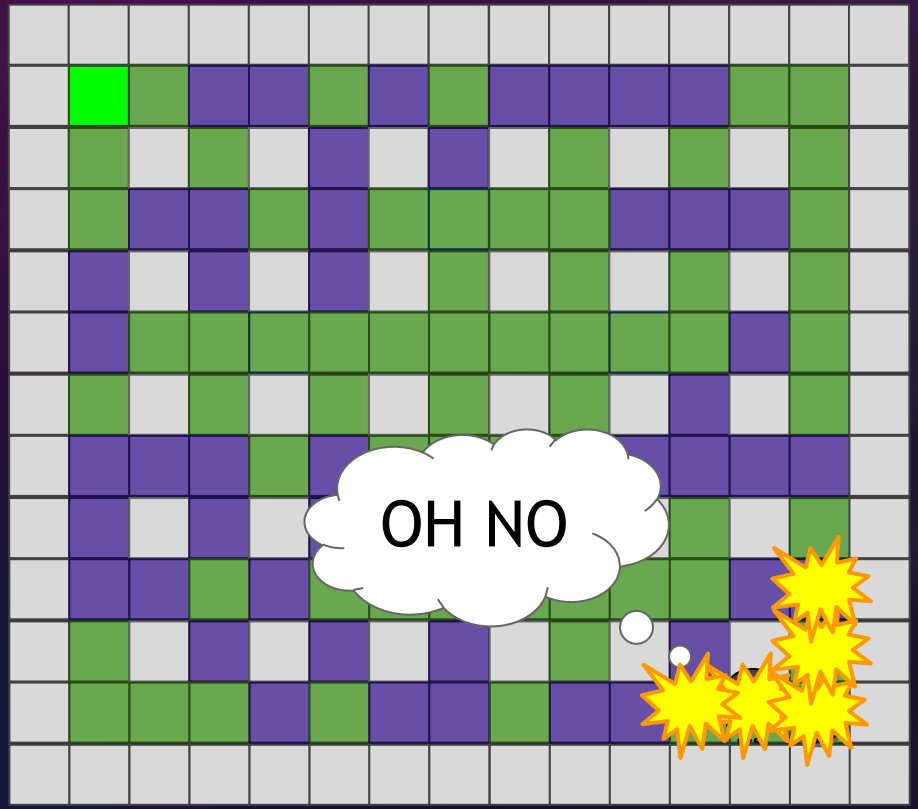
Kryteria wygranej?



Wygrywa ostatni gracz pozostający na planszy!

Ale musi jeszcze przeżyć 5 sekund (tak, żeby wszystkie bomby eksplodowały).

Kryteria wygranej?



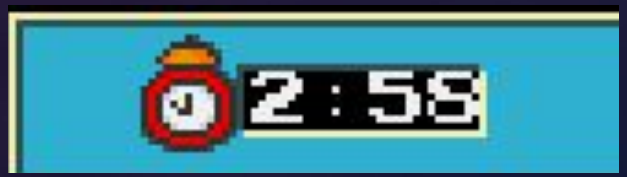
Wygrywa ostatni gracz pozostający na planszy!

Ale musi jeszcze przeżyć 5 sekund (tak, żeby wszystkie bomby eksplodowały).

Kryteria remisu?

Jeśli wszyscy gracze zginą

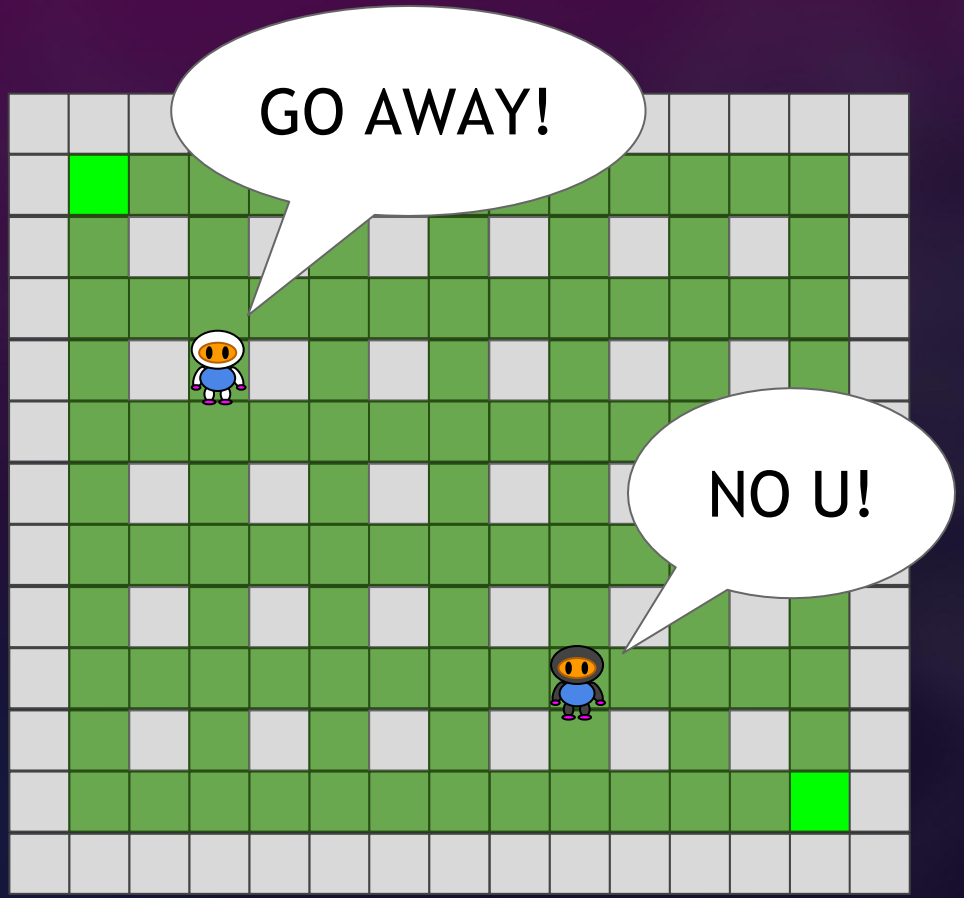
LUB



upłynie czas rundy

mamy remis!
I runda jest restartowana.

Kryteria remisu?



Zazwyczaj czas rundy się kończy gdy gracze "wyczyszczą" planszę i nie chcą mieć ze sobą nic wspólnego.

Jak wygrać remis-przez-koniec-czasu?

Technicznie mamy wszystkie informacje, jakie potrzebujemy :)
Ale, dla powtórzenia, dwa istotne szczegóły:

Jak wygrać remis-przez-koniec-czasu?

Technicznie mamy wszystkie informacje, jakie potrzebujemy :)
Ale, dla powtórzenia, dwa istotne szczegóły:

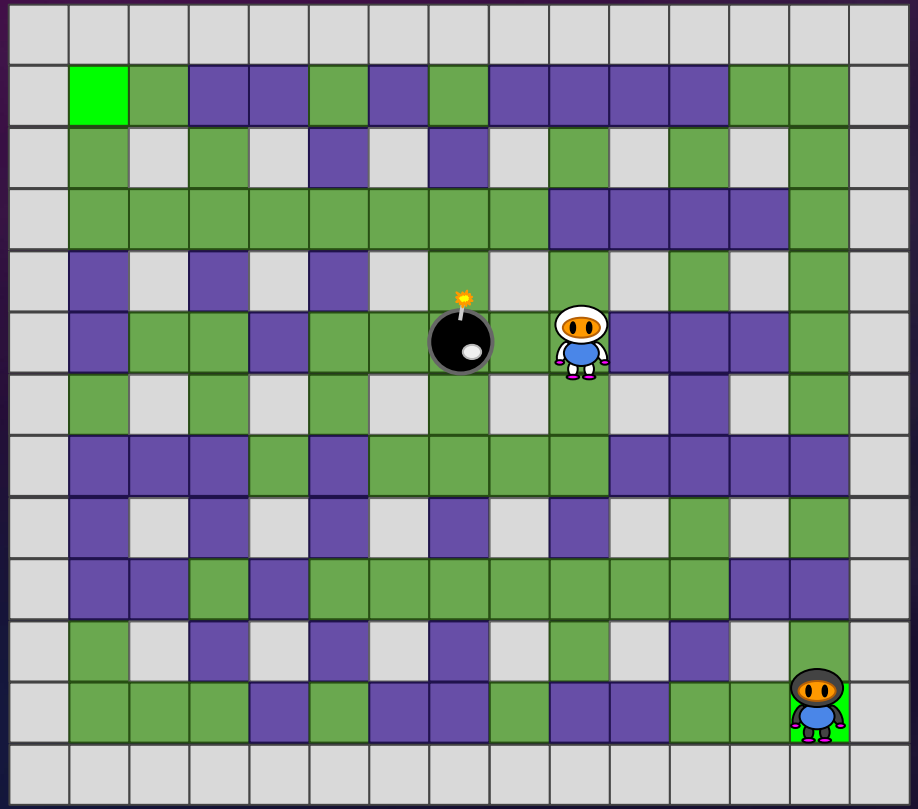
Ostatni gracz na planszy musi przeżyć jeszcze 5 sekund żeby wygrać.

Jak upłynie czas rundy, runda jest restartowana.

Myśleć jak programista

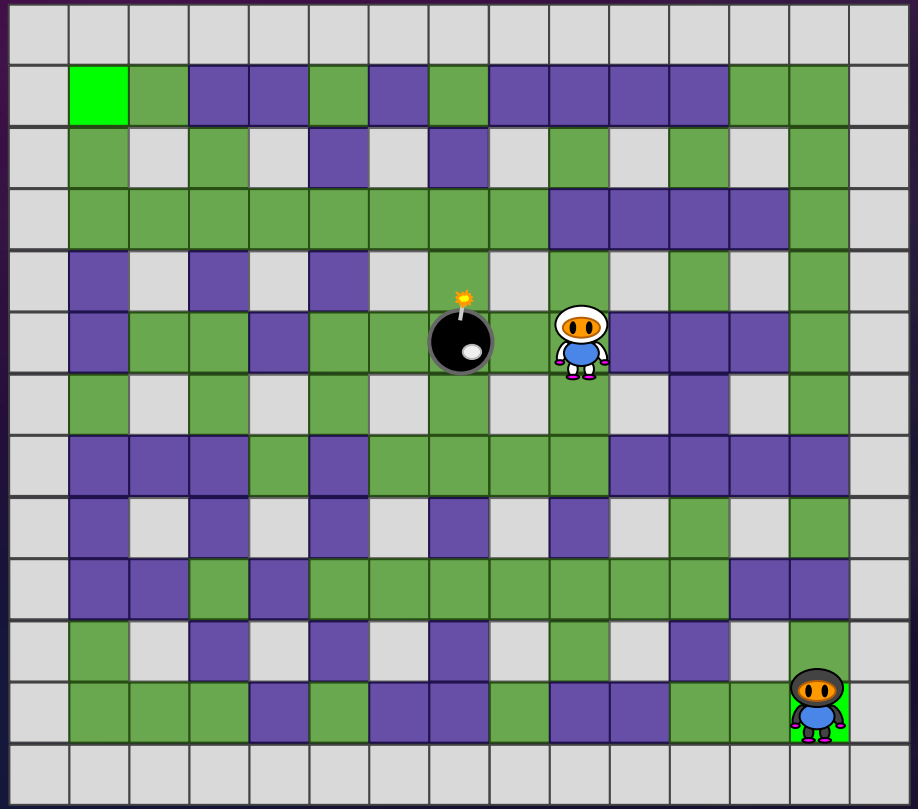
Jakie informacje musimy przechowywać o stanie gry?

Myśleć jak programista



Jakie informacje musimy przechowywać o stanie gry?

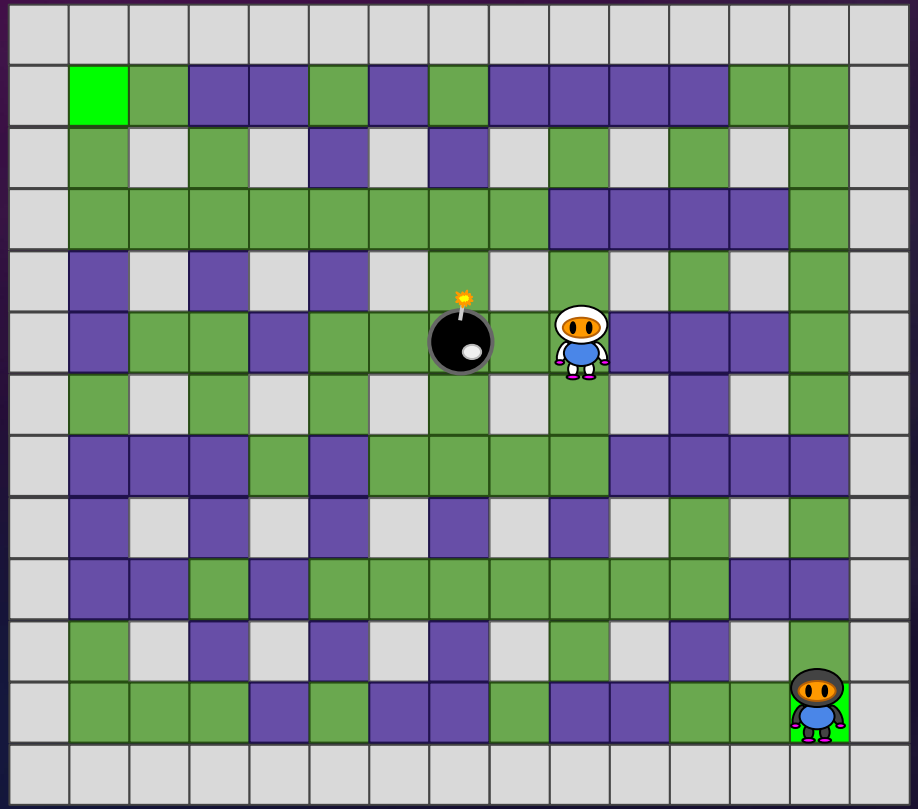
Myśleć jak programista



Jakie informacje musimy przechowywać o stanie gry?

- Pozycja gracza

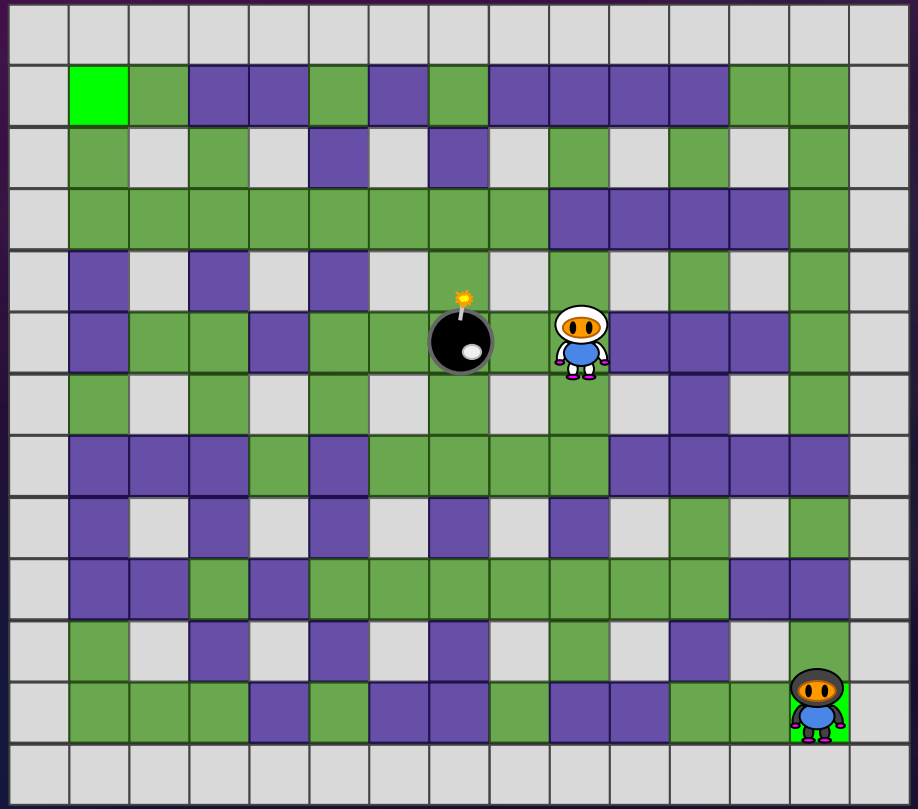
Myśleć jak programista



Jakie informacje musimy przechowywać o stanie gry?

- Pozycja gracza
- Pozycje i timer bomb

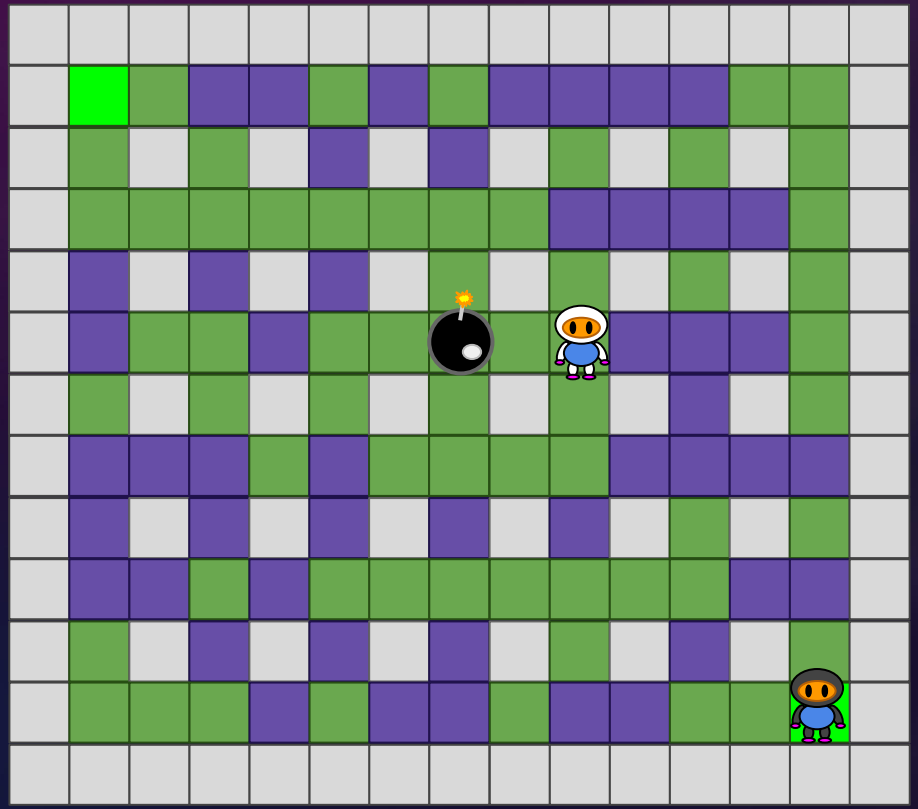
Myśleć jak programista



Jakie informacje musimy przechowywać o stanie gry?

- Pozycja gracza
- Pozycje i timer bomb
- Pozycje zniszczalnych murów

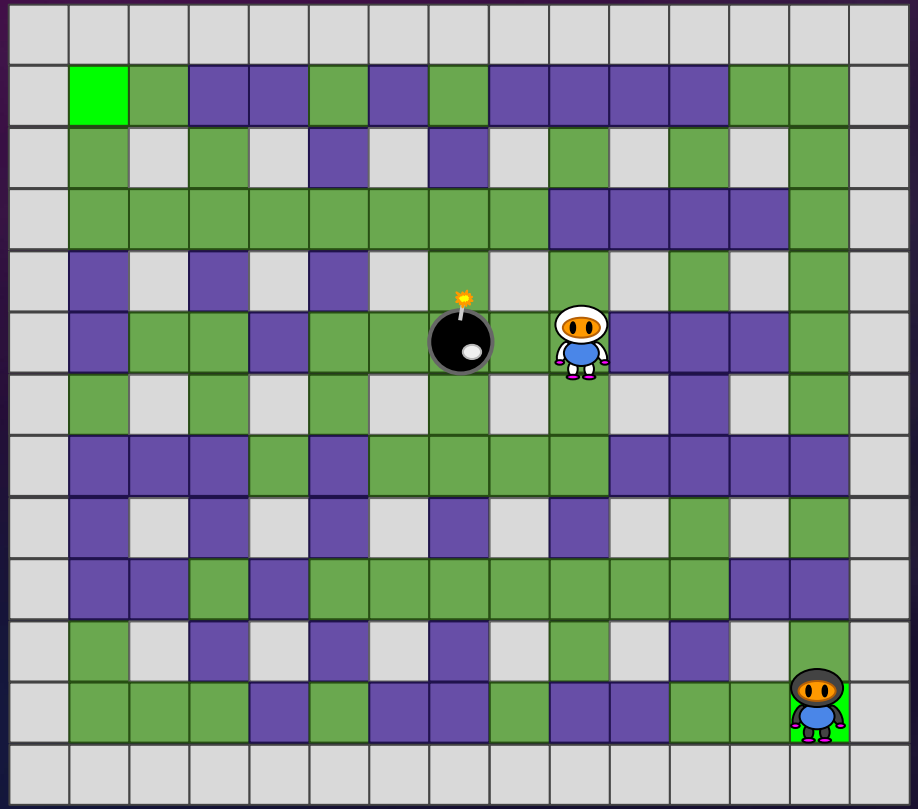
Myśleć jak programista



Jakie informacje musimy przechowywać o stanie gry?

- Pozycja gracza
- Pozycje i timer bomb
- Pozycje zniszczalnych murów
- Potwory i ich stan

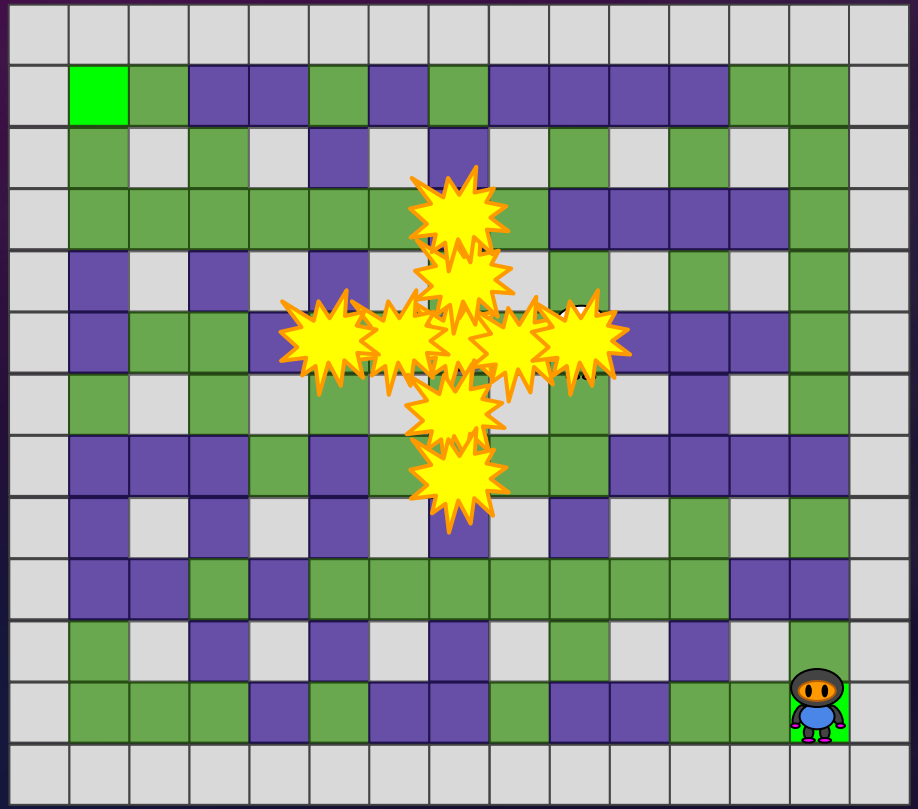
Myśleć jak programista



Jakie informacje musimy przechowywać o stanie gry?

- Pozycja gracza
- Pozycje i timer bomb
- Pozycje zniszczalnych murów
- Potwory i ich stan
- Power-upy gracza

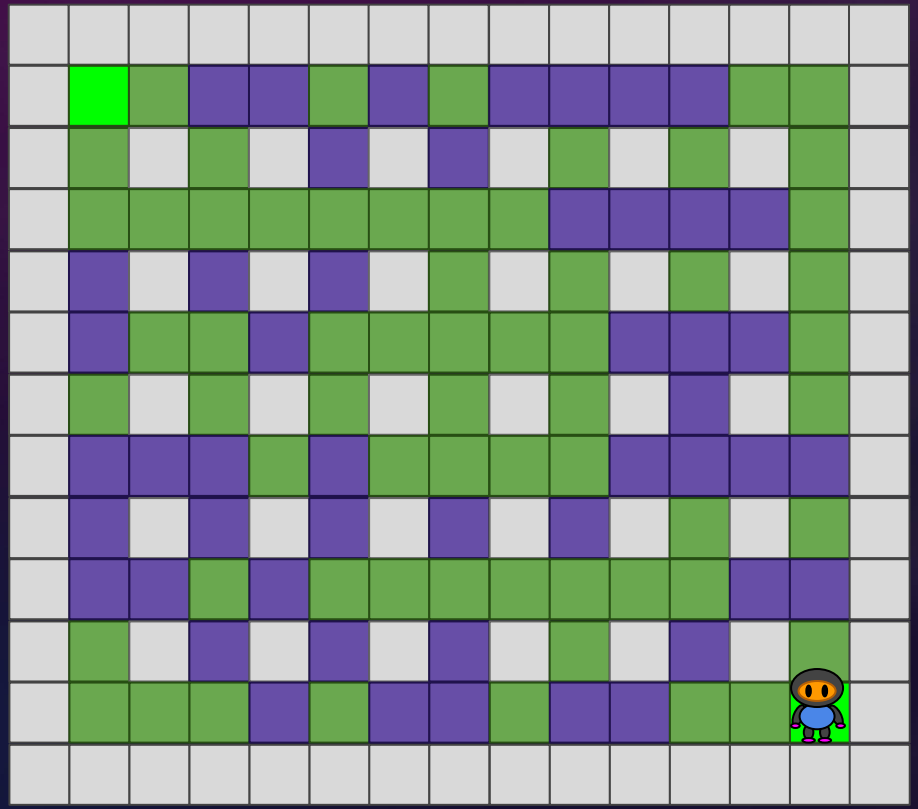
Myśleć jak programista



Jakie informacje musimy przechowywać o stanie gry?

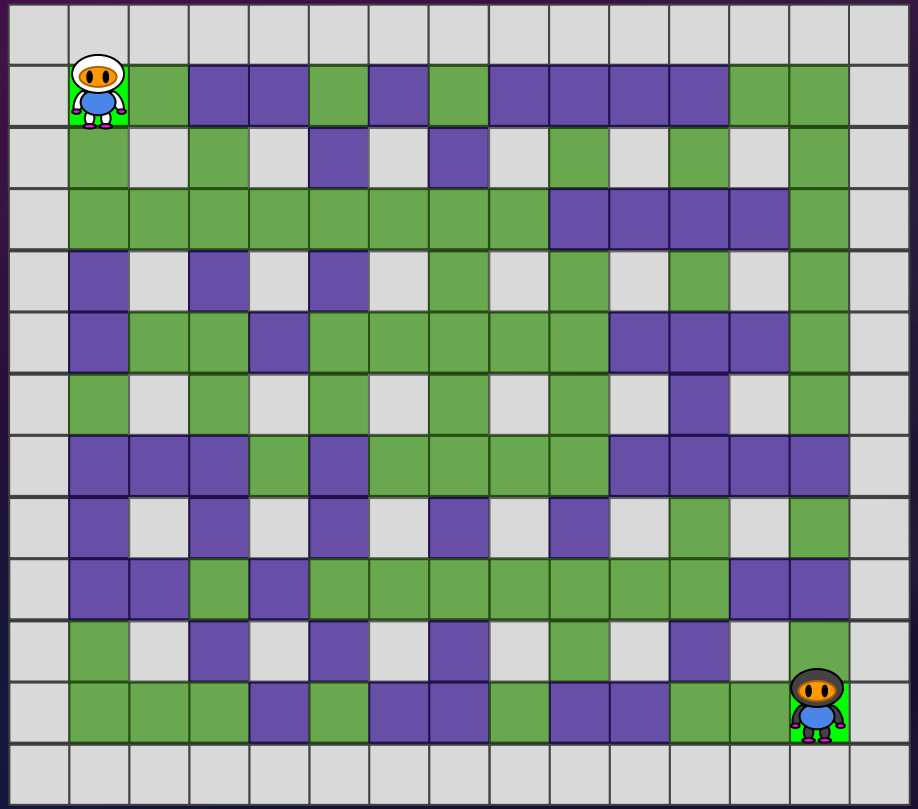
- Pozycja gracza
- Pozycje i timer bomb
- Pozycje zniszczalnych murów
- Potwory i ich stan
- Power-upy gracza

Myśleć jak programista - restart rundy



Jakie kroki trzeba podjąć, żeby zrestartować rundę?

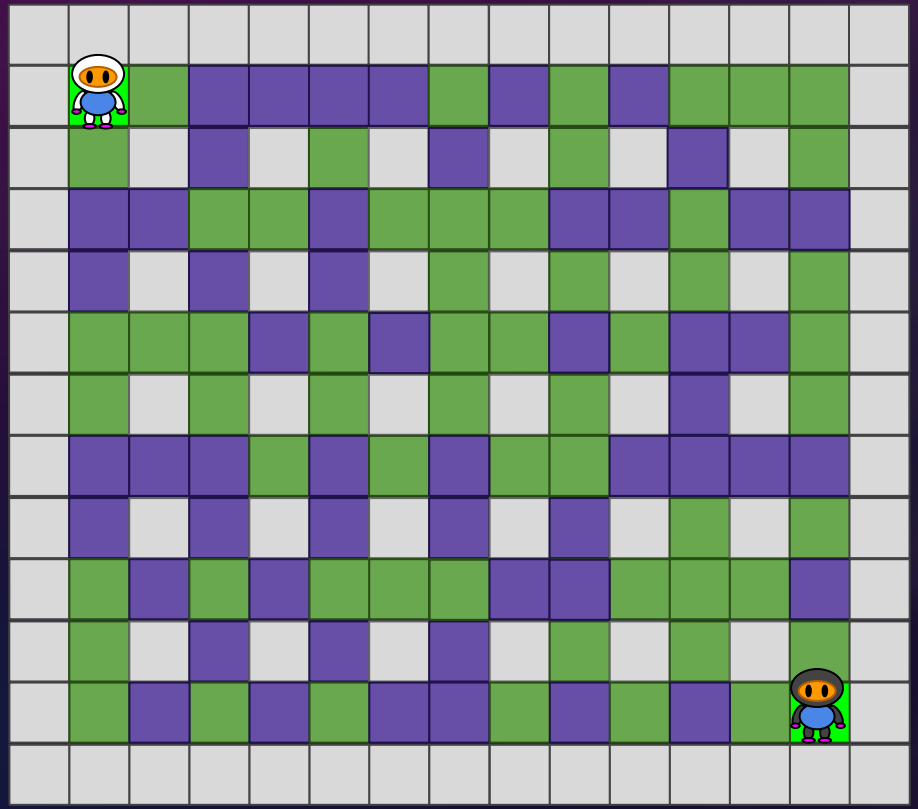
Myśleć jak programista - restart rundy



Jakie kroki trzeba podjąć, żeby zrestartować rundę?

- Pozycje graczy muszą zostać zresetowane

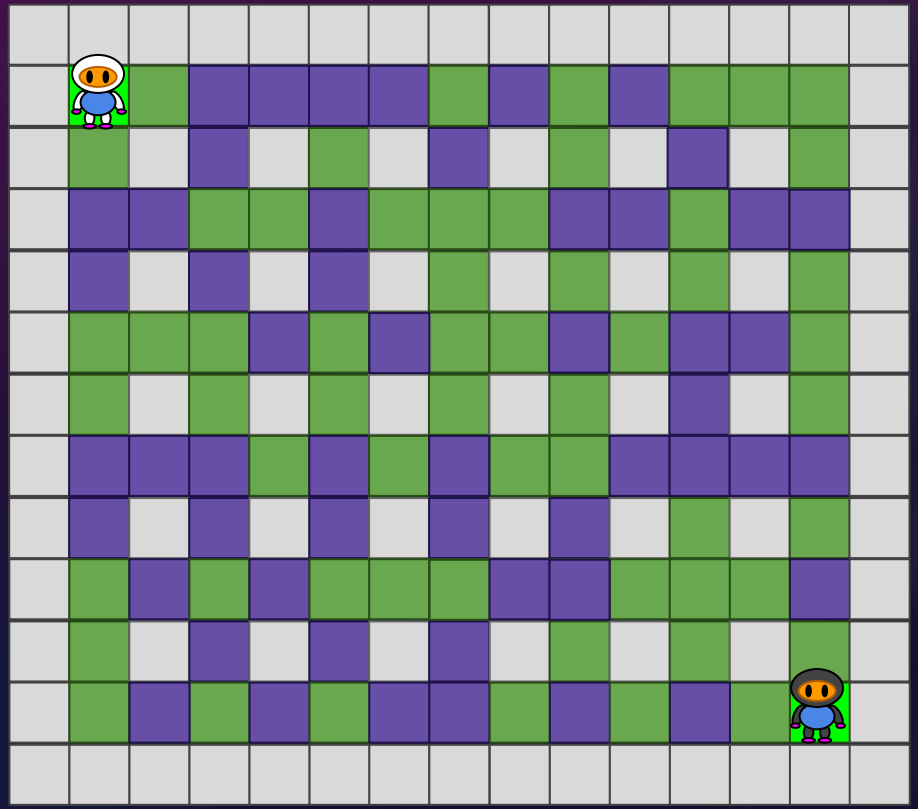
Myśleć jak programista - restart rundy



Jakie kroki trzeba podjąć, żeby zrestartować rundę?

- Pozycje graczy muszą zostać zresetowane
- Mapa musi zostać zregenerowana

Myśleć jak programista - restart rundy

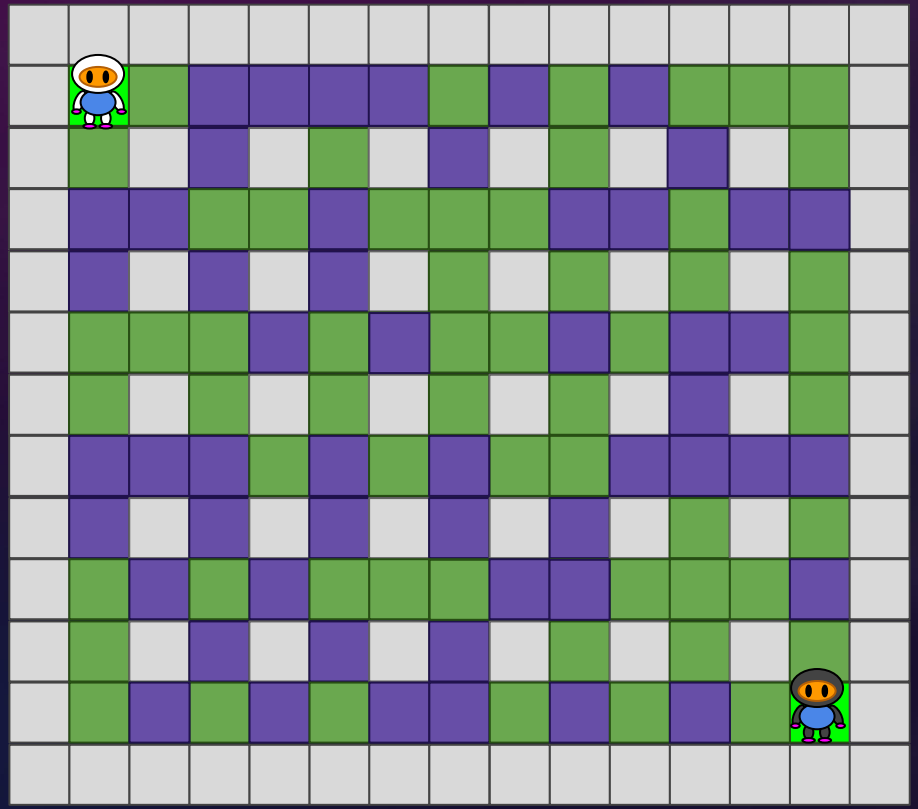


Jakie kroki trzeba podjąć, żeby zrestartować rundę?

- Pozycje graczy muszą zostać zresetowane
- Mapa musi zostać zregenerowana

W tym momencie programista może pójść przetestować kod.

Myśleć jak programista - restart rundy



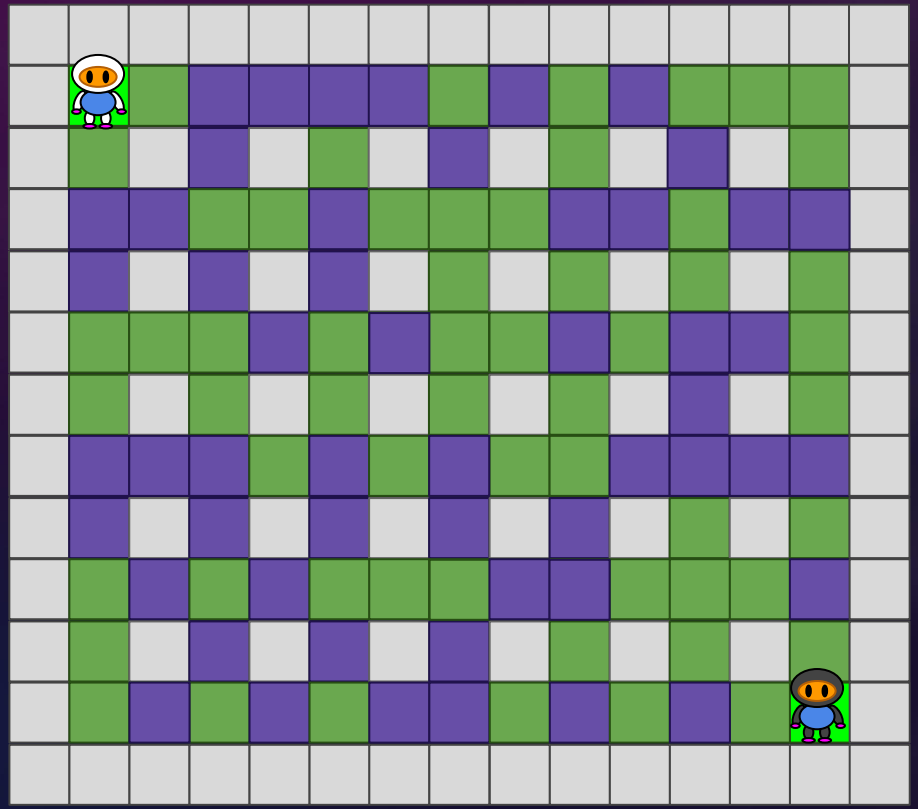
Testujemy!

Gramy ze 2 rundy

Szybko fragujemy drugiego gracza

...i zauważamy, że w kolejnej rundzie mamy power-upy niezresetowane.

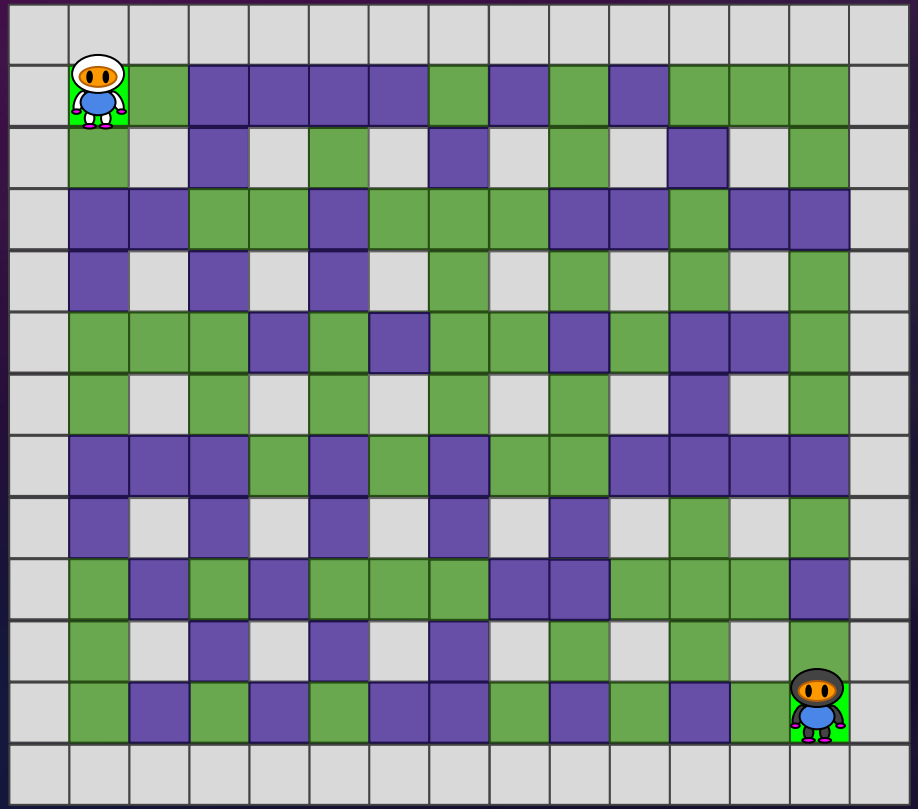
Myśleć jak programista - restart rundy



Jakie kroki trzeba podjąć, żeby zrestartować rundę?

- Pozycje graczy muszą zostać zresetowane
- Mapa musi zostać zregenerowana
- Stan power-upów graczy musi zostać wyzerowany

Myśleć jak programista - restart rundy



Testujemy #2:

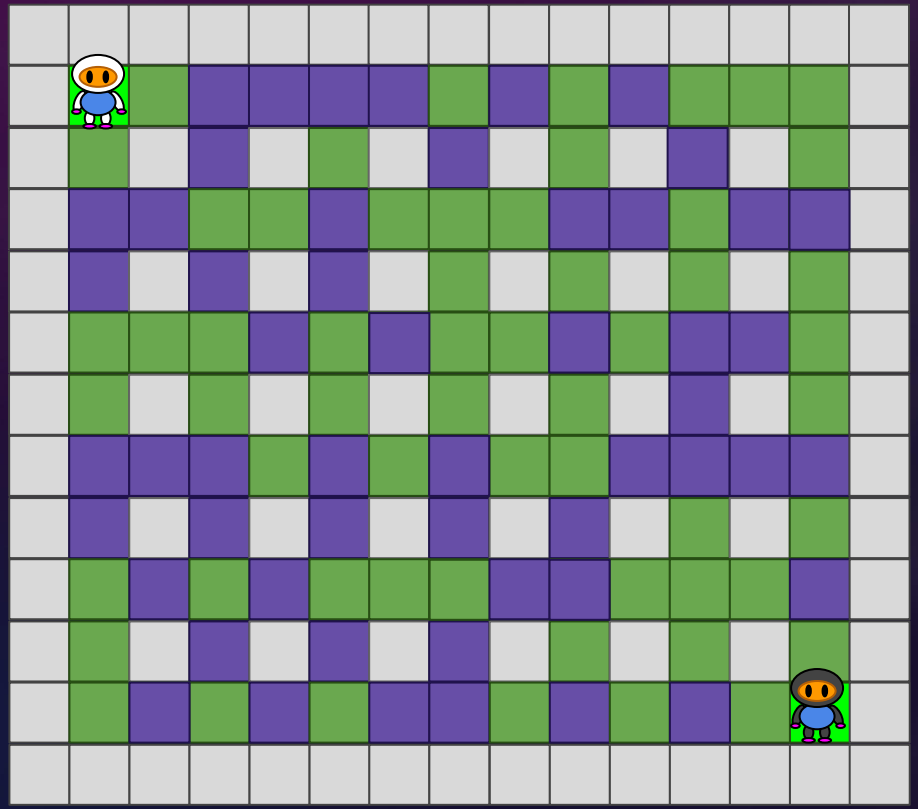
Gramy ze 2 rundy.

Szybko fragujemy nieruchomego gracza.

Wszystko chyba działa.

Grę kartonik i do sklepu!

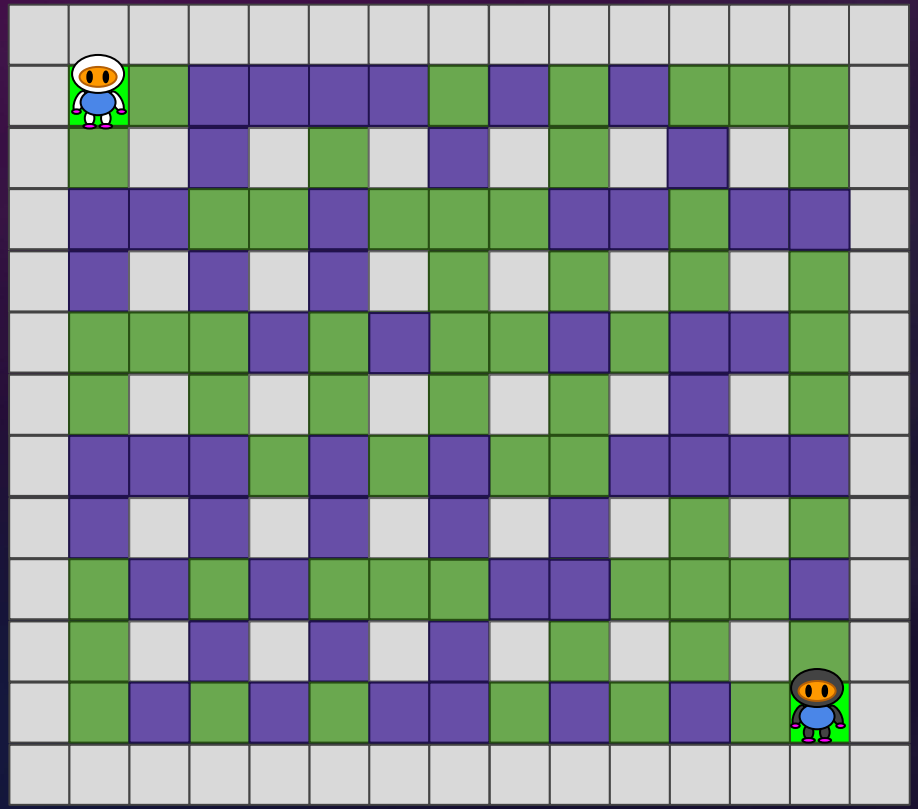
Myśleć jak programista - restart rundy



Co programista przeoczył?

???

Myśleć jak programista - restart rundy



Co programista przeoczył?

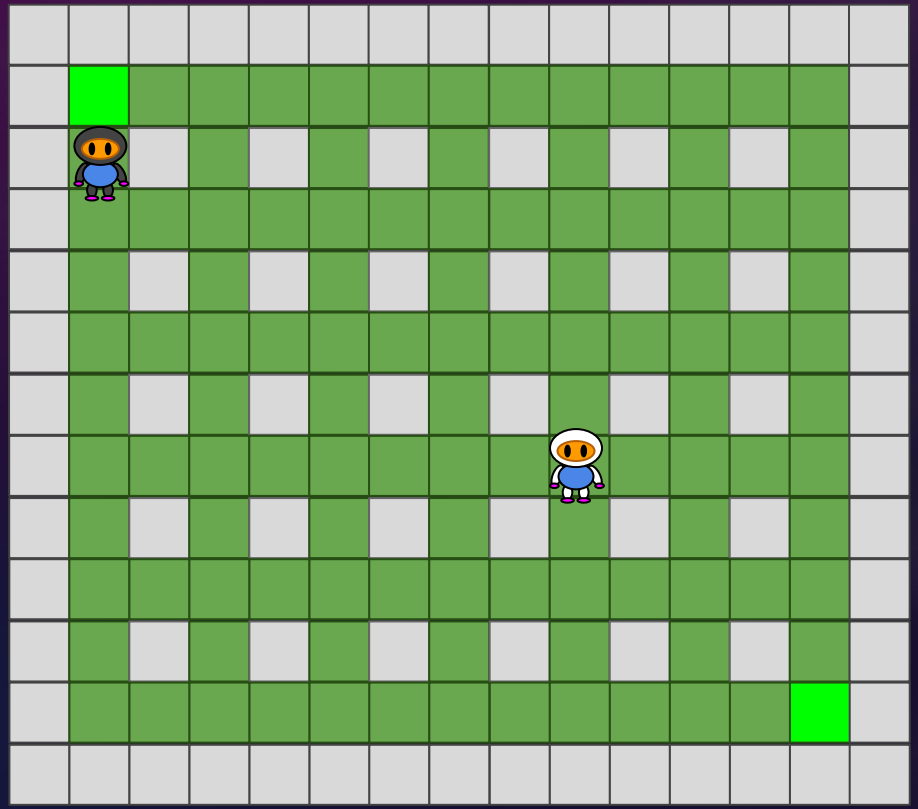
Zresetowanie stanu bomb na planszy.

Protip

Szukając błędów posadź się na miejscu
(zmęczonego) programisty lub sysadmina

Jak to wykorzystać?

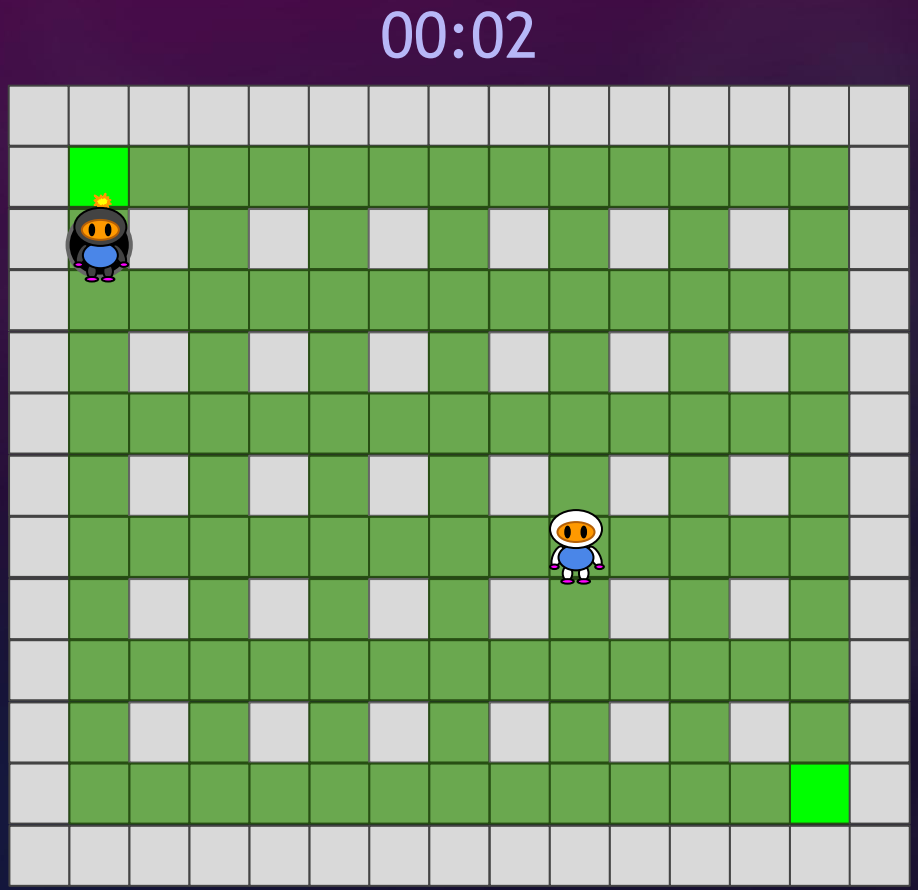
00:02



Jak czas pokazuje około 0:02,

połóż bombę lub pięć na respawnie swojego przeciwnika.

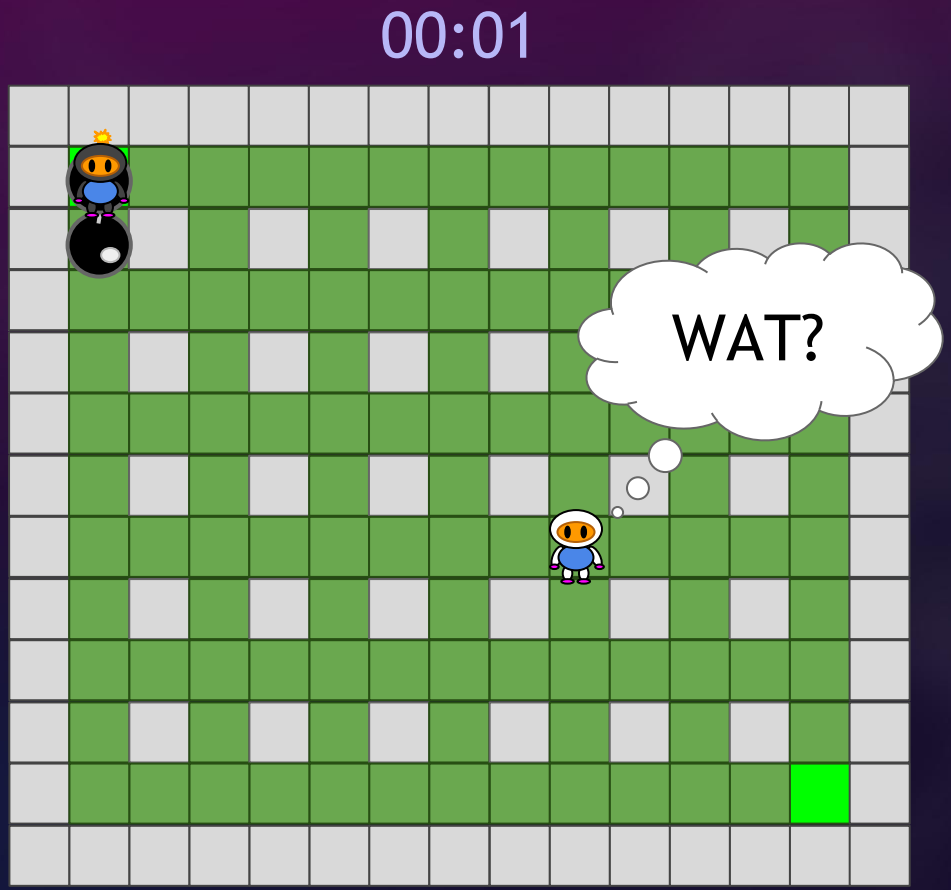
Jak to wykorzystać?



Jak czas pokazuje około 0:02,

połóż bombę lub pięć na respawnie swojego przeciwnika.

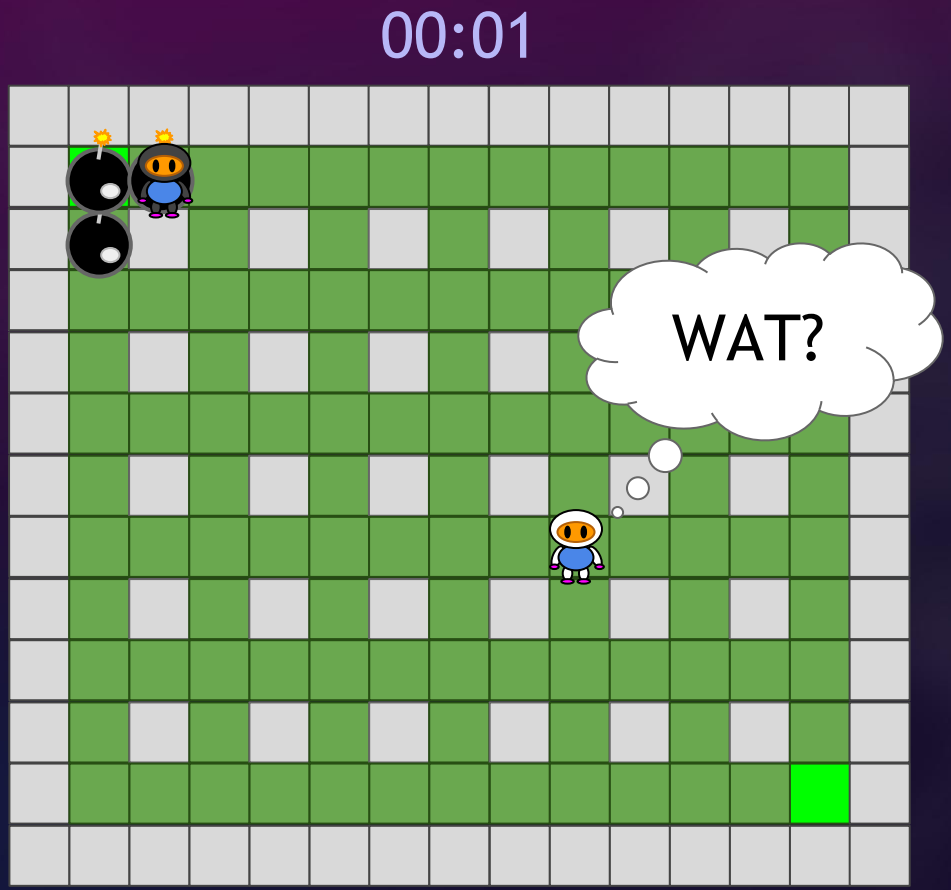
Jak to wykorzystać?



Jak czas pokazuje około 0:02,

połóż bombę lub pięć na respawnie swojego przeciwnika.

Jak to wykorzystać?

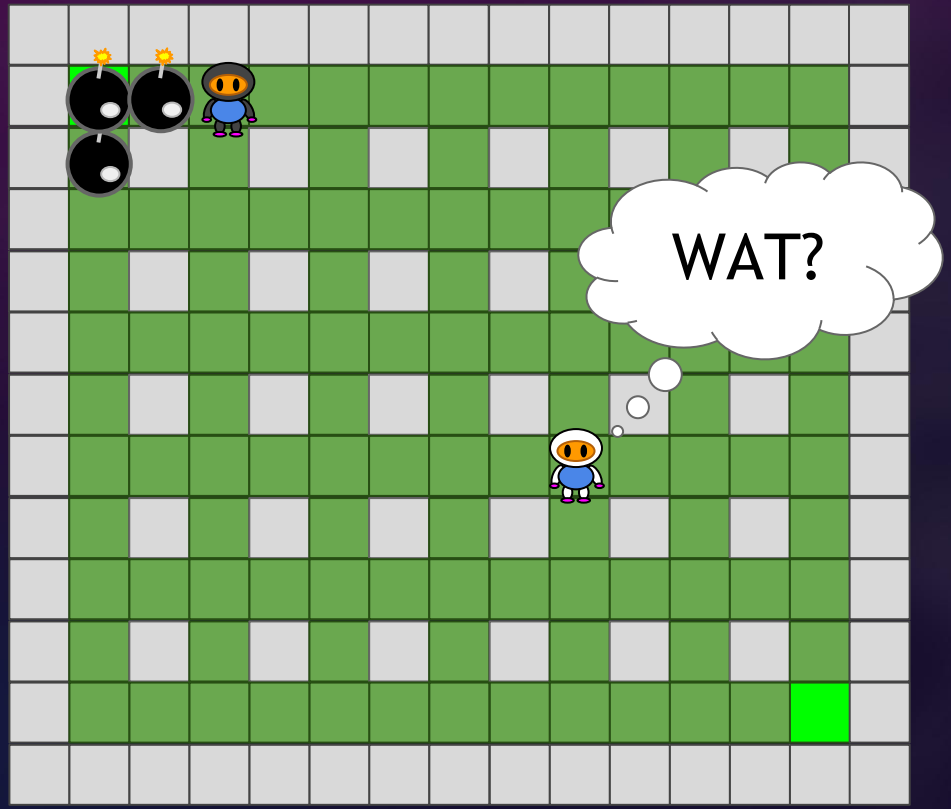


Jak czas pokazuje około 0:02,

połóż bombę lub pięć na respawnie swojego przeciwnika.

Jak to wykorzystać?

00:00



Jak czas pokazuje około 0:02,

połóż bombę lub pięć na respawnie swojego przeciwnika.

Jak to wykorzystać?

Obejrzyj ekran remisu.

Odłóż kontroler.

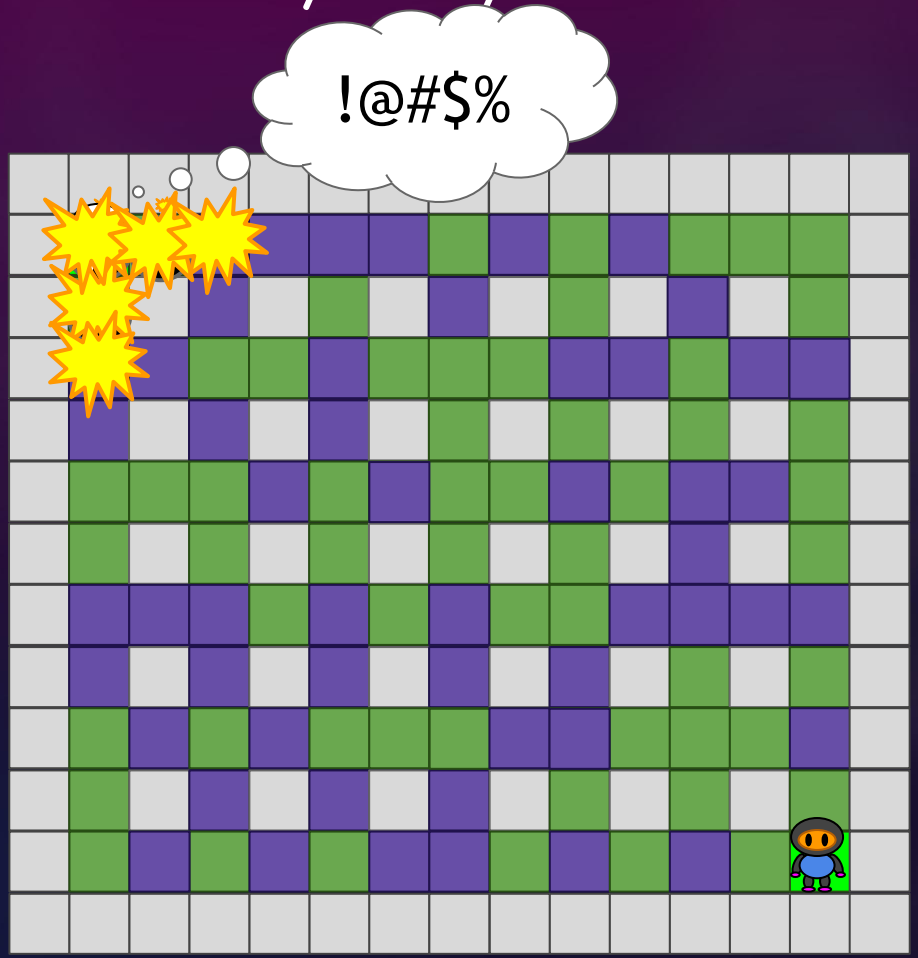
Weź łyka herbaty.

Powiedz:
"It's over Anakin, I have the high ground!"

Jak to wykorzystać?

Wygraj rundę.

Jak to wykorzystać?



Wygraj rundę.

(Zazwyczaj można to użyć kilka razy zanim przeciwnik się zorientuje co się dzieje)

Protip

Często nie chodzi o to co JEST w kodzie
tylko o to czego w kodzie BRAKUJE

Stukanie klawiatury

Szczegóły na przykładach #2

Stukanie klawiatury

Czy jeśli ktoś by nagrał nas kamerą
jak wpisujemy nasze hasło,
to czy można nasze hasło z nagrania wyciągnąć?

Stukanie klawiatury

Czy jeśli ktoś by nagrał nas kamerą
jak wpisujemy nasze hasło,
to czy można nasze hasło z nagrania wyciągnąć?

Jasne, że TAK

Stukanie klawiatury

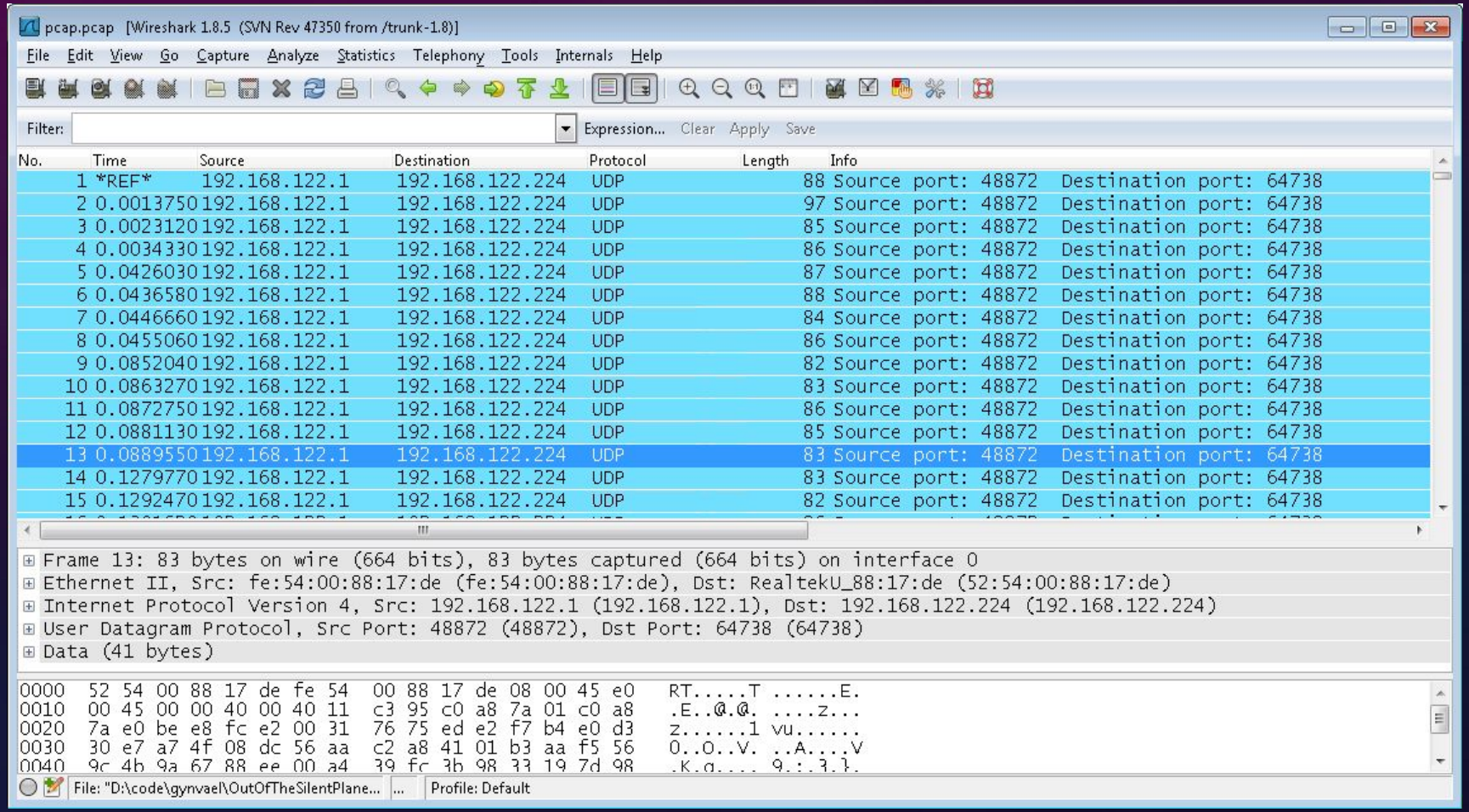
Czy jeśli ktoś by nagrał nas kamerą
jak wpisujemy nasze hasło,
to czy można nasze hasło z nagrania wyciągnąć?

Jasne, że TAK

A co jeśli nie będzie obrazu?
Tj. będzie tylko dźwięk?

Dygresja - Mumble mumble (BKP2013)

PCAP z komunikacji via Mumble



Huston, mamy problem

Mumble uses the low-latency audio codec Opus as of version 1.2.4,[6] the codec that succeeds the previous defaults Speex and CELT.

Mumble connects to a server via a TLS control channel, with the audio travelling via UDP encrypted with AES in OCB mode.

Źródło: https://en.wikipedia.org/wiki/Mumble_(software)

Huston, mamy problem

Mumble uses the low-latency audio codec Opus as of version 1.2.4,[6] the codec that succeeds the previous defaults Speex and CELT.

Mumble connects to a server via a TLS control channel, with the audio travelling via UDP encrypted with AES in OCB mode.

Nie posiadamy kluczy do szyfru.
Do dyspozycji mamy tylko zaszyfrowane pakiety UDP.

Źródło: https://en.wikipedia.org/wiki/Mumble_(software)

Czyli, mieliśmy tyle

Blob* zaszyfrowanych danych

Co spróbowaliśmy...

- Znaleźć bug w kodzie sieciowym Mumble

Co spróbowaliśmy...

- Znaleźć bug w kodzie krypto w Mumble

Co spróbowaliśmy...

- Odszukać publiczne ataki na tryb AES-OCB:
  "Niels Ferguson pointed out collision attacks on OCB, which limits the amount of data that can be securely processed under a single key to about 280 terabytes."
  Źródło: https://en.wikipedia.org/wiki/OCB_mode

Co spróbowaliśmy...

- Sprawdzić, czy w pakietach sieciowych nie ma jakichś wycieków z pamięci Mumble

Co spróbowaliśmy...

- Sprawdzić czy może klucze są generowane jakimś niekoniecznie bezpiecznym generatorem liczb losowych.

Co spróbowaliśmy...

- ... albo seed jest źle generowany.

Protip

Jeśli się utknie,
to czasem warto
zacząć od początku

Co spróbowaliśmy...

- Znowu zaczęliśmy szukać JAKIEGOKOLWIEK związanego z zadaniem buga w Mumble

Co spróbowaliśmy...

- I przejrzeliśmy cały PCAP w poszukiwaniu jakichkolwiek bajtów niewiadomego pochodzenia.

I nic z tego nie wyszło

Wynik naszych starań: Nada.

Protip

Jeśli się utknie,
to czasem warto
zrobić sobie krótką przerwę

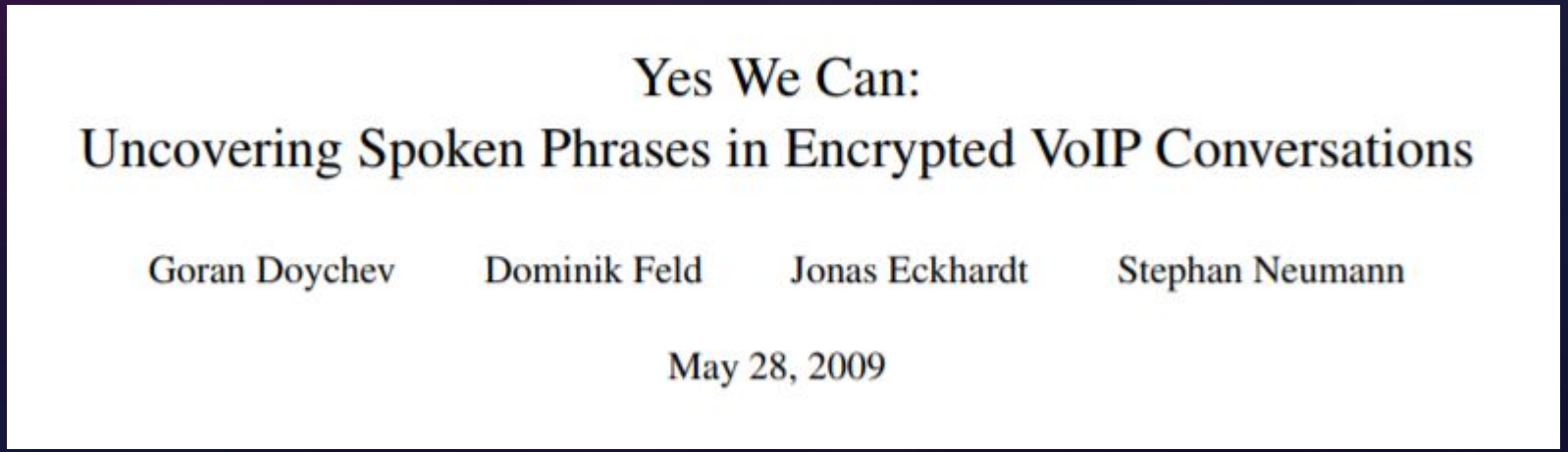
Protip

Jeśli się utknie przy problemie, o którym wiadomo,
że jest rozwiązywalny, to czasem warto,
pomyśleć jak trzeba by zbudować taki twór,
żeby dało się go rozwiązać.

Eureka! Pewien stary papierek...

"Yes We Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations"

Goran Doychev, Dominik Feld, Jonas Eckhardt, Stephan Neumann



Yes We Can:
Uncovering Spoken Phrases in Encrypted VoIP Conversations

Goran Doychev Dominik Feld Jonas Eckhardt Stephan Neumann

May 28, 2009

Protip

Warto czytać publikacje naukowe z naszej działki ;).
(choćby i sam abstract)

(a btw, wrzućcie w google "ciekawe-papierki")

To stwierdzenie by było prawdziwe dla pliku, ale my mieliśmy PCAP...

~~Blob* zaszyfrowanych danych~~

A to oznacza, że mieliśmy pakiety.

Oraz ich rozmiary.

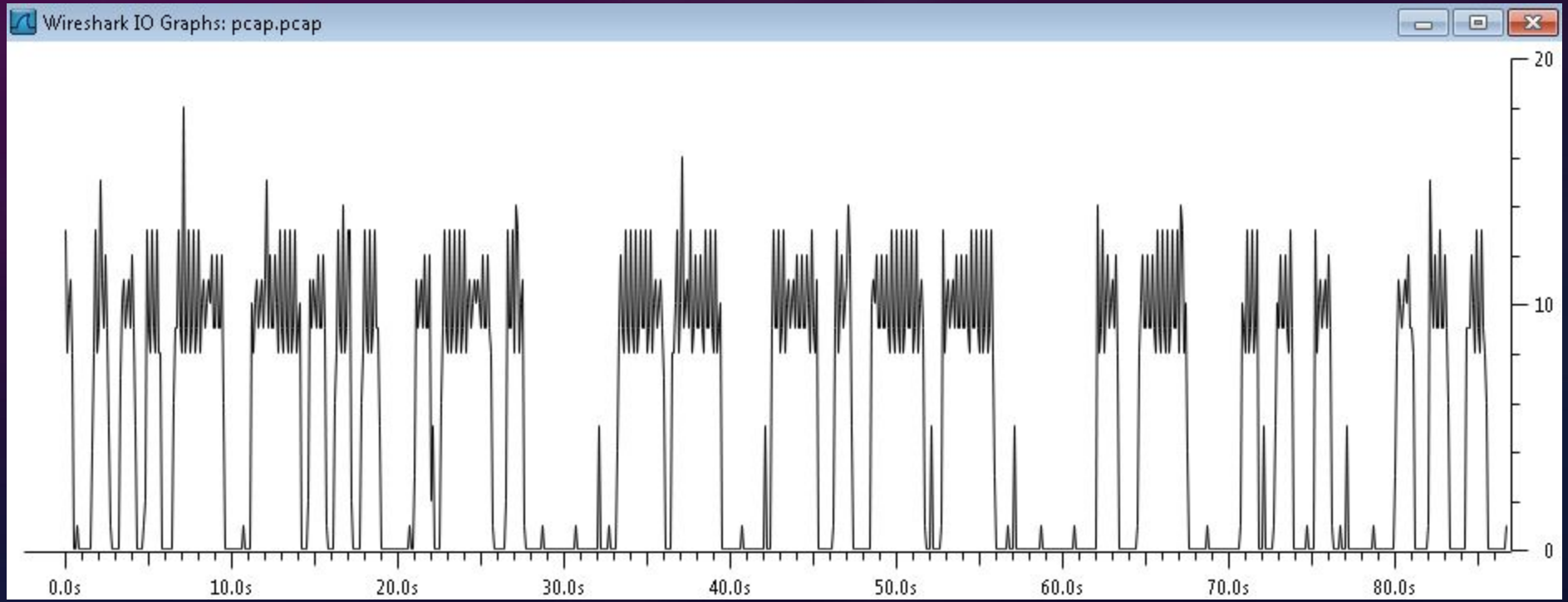
Oraz czas nadania/odbioru

VBR - Variable Bit Rate

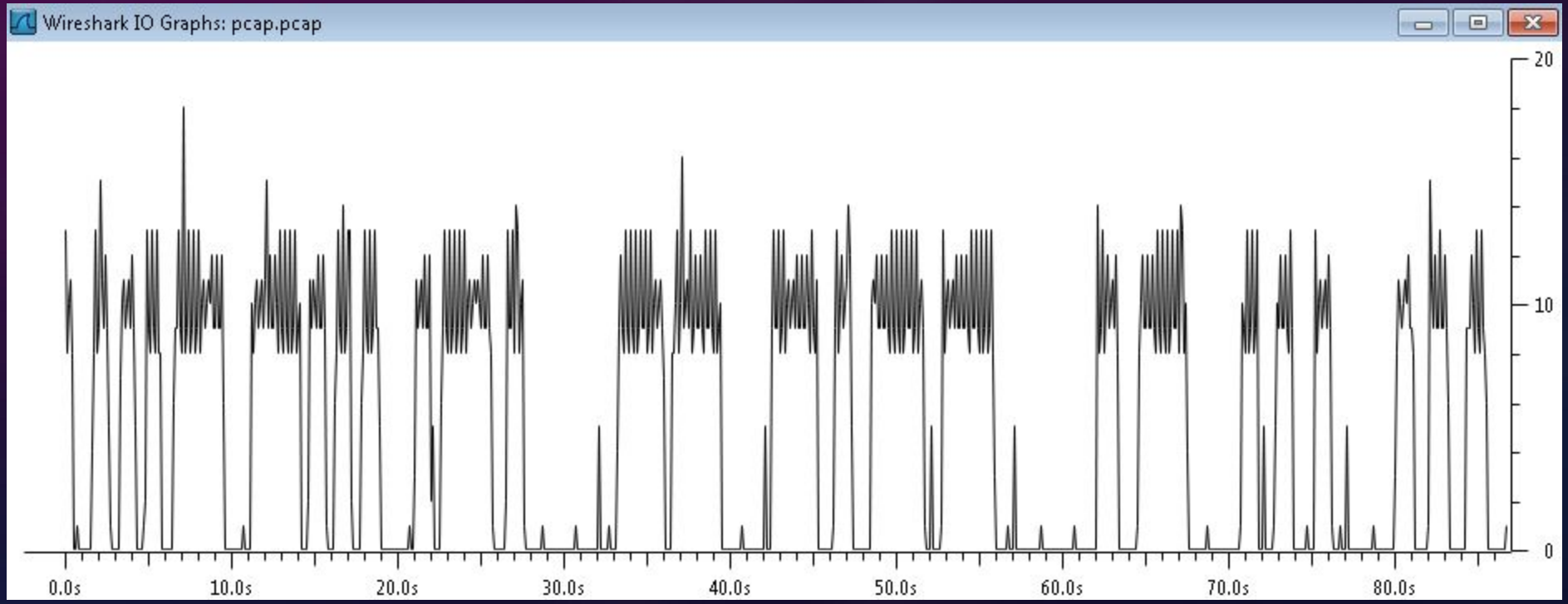
W komunikacji audio z VBR:

- cisza nie musi być wysyłana (bitrate 0)
- aktywne mówienie / dźwięk odpowiednio podnosi bitrate

Wykres na podstawie PCAP (poziom: "EASY")



Zdekodowanie reszty pozostawiam jako ćwiczenie



...-	-...	.-.	--	-.--	.-	...	...
V	B	R	M	Y	A		

Wróćmy do nagrania klawiatury

Posiadając takie nagranie...

Wiemy DOKŁADNIE kiedy dany klawisz został naciśnięty.

I to z całkiem niezłą rozdzielczością:

- 44100 Hz (CD quality) → 22.6 us
- 48000 Hz (DVD quality) → 20.8 us

Okazuje się, że jak poruszamy palcami, to one się poruszają

Uhm, to znaczy, fizycznie się poruszają.

Okazuje się, że jak poruszamy palcami, to one się poruszają

Oczywiście trzeba wziąć pod uwagę też...

- Rozmiar i model klawiatury
- Indywidualne cechy danej osoby (profil/model)
- Nastrój ;)
  - ("Somebody is wrong on the internet!" *prędkość wzrasta*)
- Ile próbek/danych mamy do dyspozycji

Niemniej jednak da się to zrobić

Timing Analysis of Keystrokes and Timing Attacks on SSH

Dawn Xiaodong Song, David Wagner, Xuqing Tian

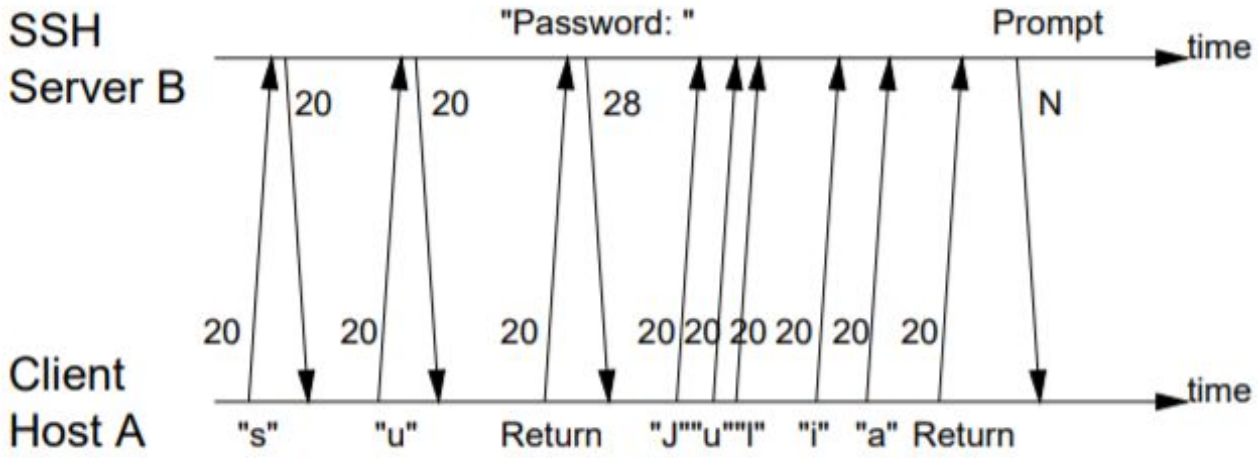


Figure 1: The traffic signature associated with running `SU` in a `SSH` session. The numbers in the figure are the size (in bytes) of the corresponding packet payloads.

Wróćmy do przysłowiowego słonia w pokoju

Chwila, przecież mamy nagranie AUDIO!

Okazuje się, że każdy klawisz brzmi trochę inaczej...

=

?

Ponownie, zostało to udowodnione i poprawione

Keyboard Acoustic Emanations

Dmitri Asonov, Rakesh Agrawal

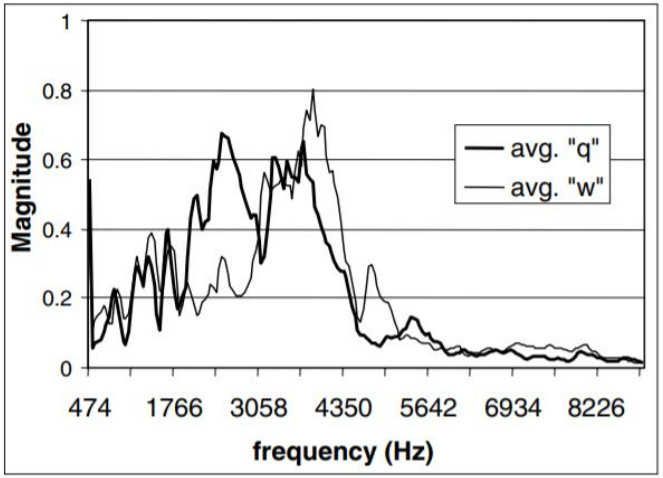


Figure 5. Comparison of the normalized average spectrums (extracted from touch peaks of the clicks).

Keyboard A, ADCS: 1.99						
key pressed	q	w	e	r	t	y
recognized	9,0,0	9,1,0	1,1,1	8,1,0	10,0,0	7,1,0
key pressed	u	i	o	p	a	s
recognized	7,0,2	8,1,0	4,4,1	9,1,0	6,0,0	9,0,0
key pressed	d	f	g	h	j	k
recognized	8,1,0	2,1,1	9,1,0	8,1,0	8,0,0	8,0,0
key pressed	l	;	z	x	c	v
recognized	9,1,0	10,0,0	9,1,0	10,0,0	10,0,0	9,0,1
key pressed	b	n	m	,	.	/
recognized	10,0,0	9,1,0	9,1,0	6,1,0	8,1,0	8,1,0

Table 2. The neural network is tested with 300 clicks, 10 clicks per key.

that a click is produced by the key k (l) if it assigns an output node a value between 0 and 0.5 (0.5 and 1). The

Ponownie, zostało to udowodnione i poprawione

Keyboard Acoustic Emanations Revisited
Li Zhuang, Feng Zhou, J. D. Tygar

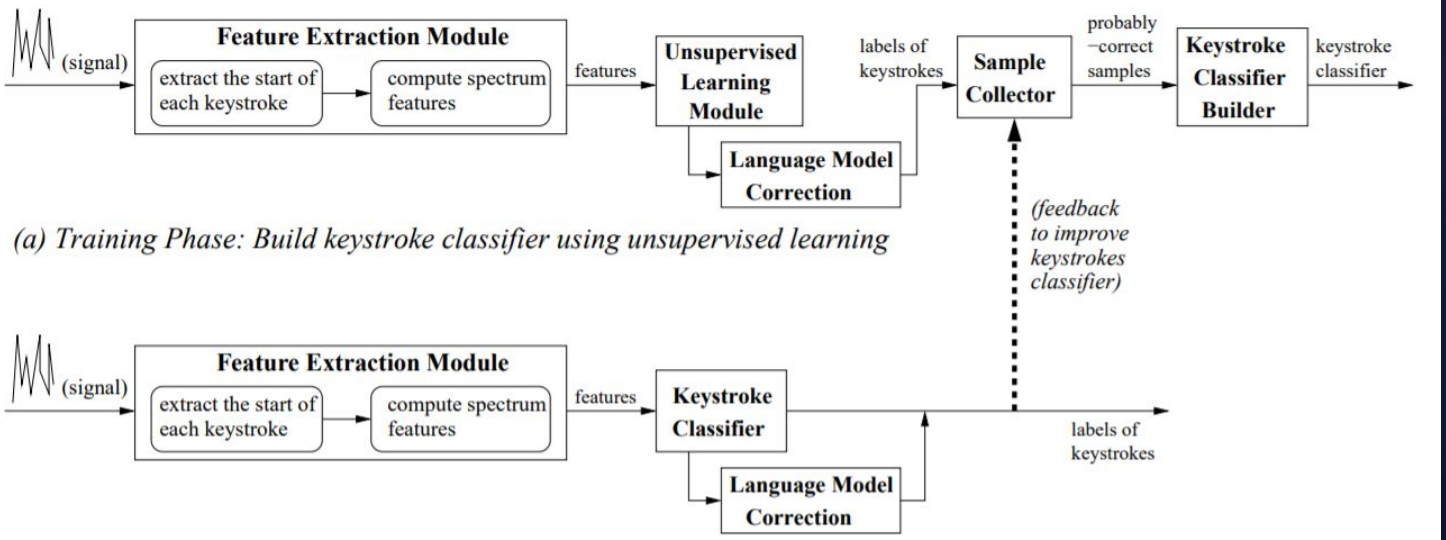


Figure 2: Overview of the attack.

Ponownie, zostało to udowodnione i poprawione

Cracking Passwords using Keyboard Acoustics and Language Modeling

Andrew Kelly (Master's Thesis, 2010)

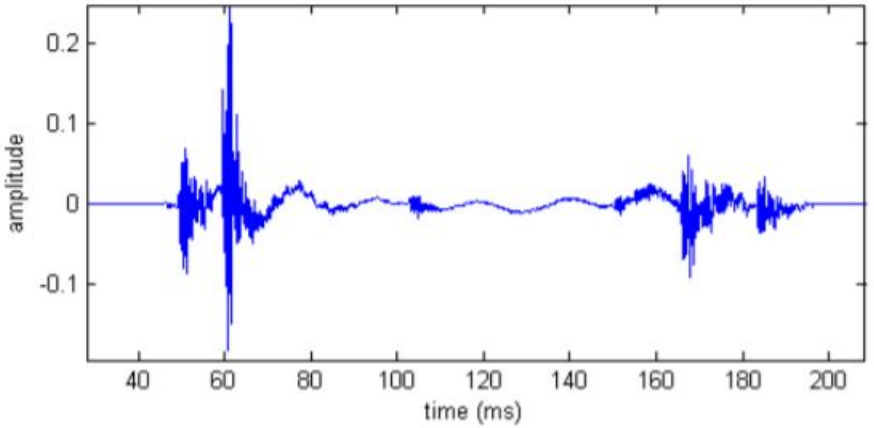


Figure 2.1: Audio signal of a single keystroke

Linie energetyczne i PS/2

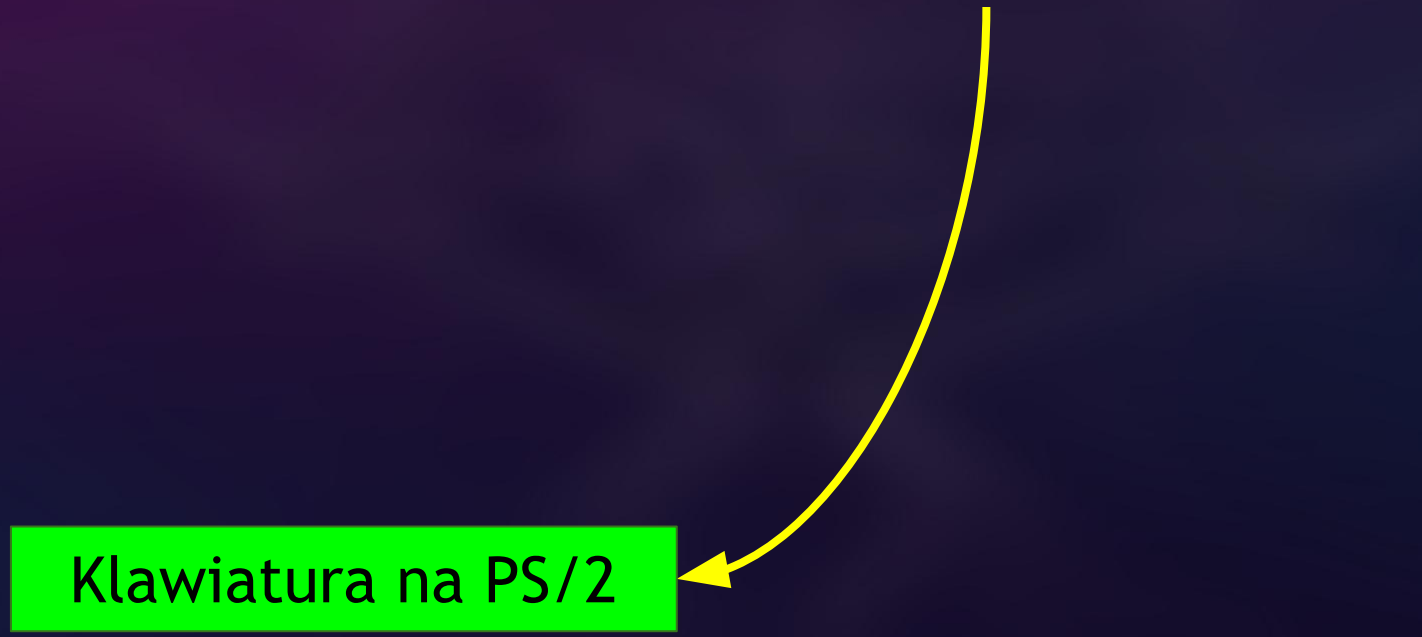
Komputer

Klawiatura na PS/2

Aparatura pomiarowa

Linie energetyczne i PS/2

Ktoś tu jeszcze takiej używa?



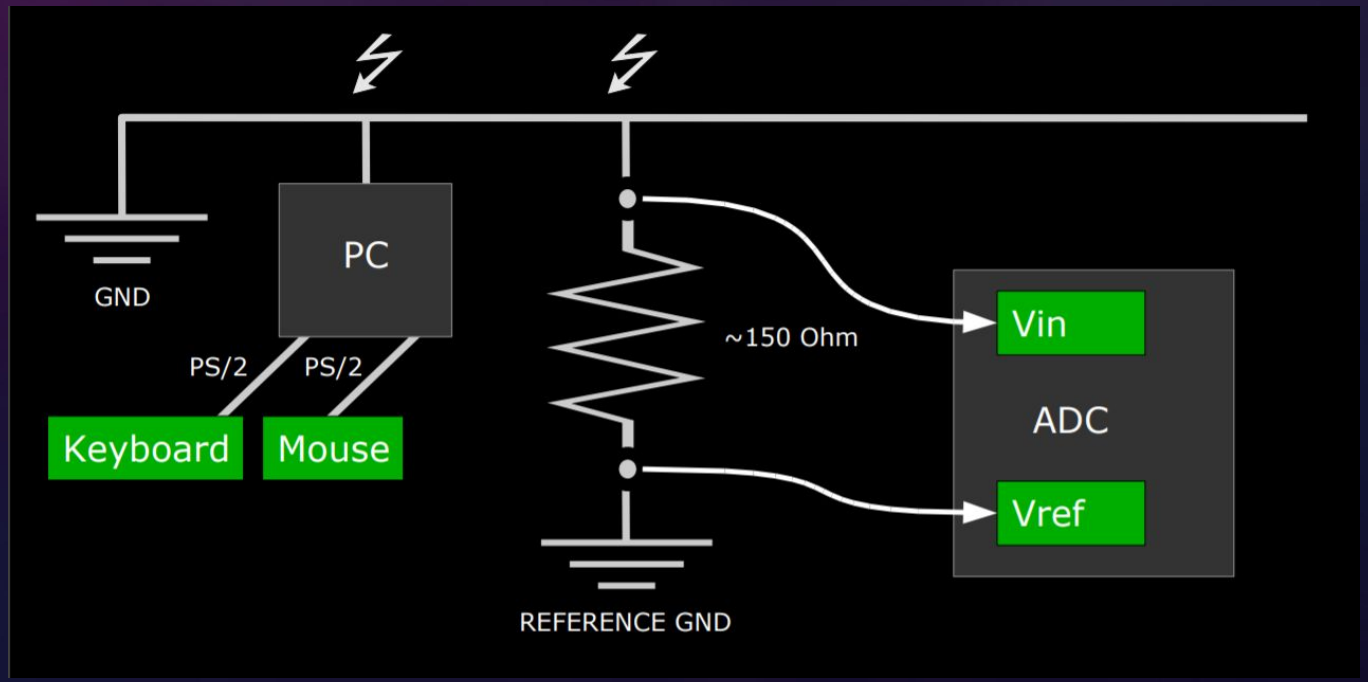
Linie energetyczne i PS/2

Linie energetyczne i PS/2

Sniffing Keystrokes With Lasers/Voltmeters

Andrea Barisani, Daniele Bianco

ATMs



No i jest jeszcze TEMPEST i przyjaciele...

Aparatura pomiarowa z anteną

Ulot Elektromagnetyczny

No i jest jeszcze TEMPEST i przyjaciele...

Compromising Electromagnetic Emanations of Wired and Wireless Keyboards

Martin Vuagnoux, Sylvain Pasini

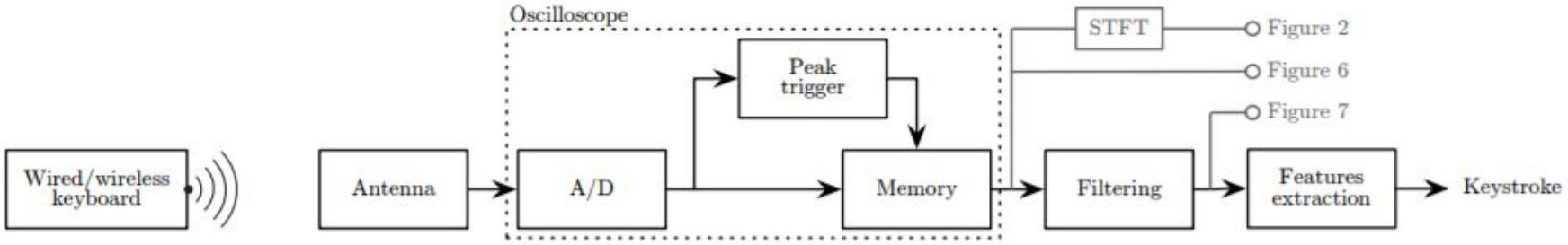


Figure 1: Diagram of our equipment for the experiments.

Klawiatura i side-channel - podsumowanie

- Czas naciśnięcia
- Dźwięk klawiszy
- Linie energetyczne
- Ulot elektromagnetyczny

About that (il)legal hacking

Szczegóły na przykładach #4

Protip

If you're interested in security/hacking

DO read and know the law

Protip

If you're interested in security/hacking

DO read and know the law

Wait.
Which country's law?

Protip

If you're interested in security/hacking
DO read and know the law

User from country A is using a service in country B owned by company from country C and their account is accessed by a person from country D.

Wait.
Which country's law?

Protip

Reading legal papers is actually very similar to reading formal protocol documentation

(especially RFC)

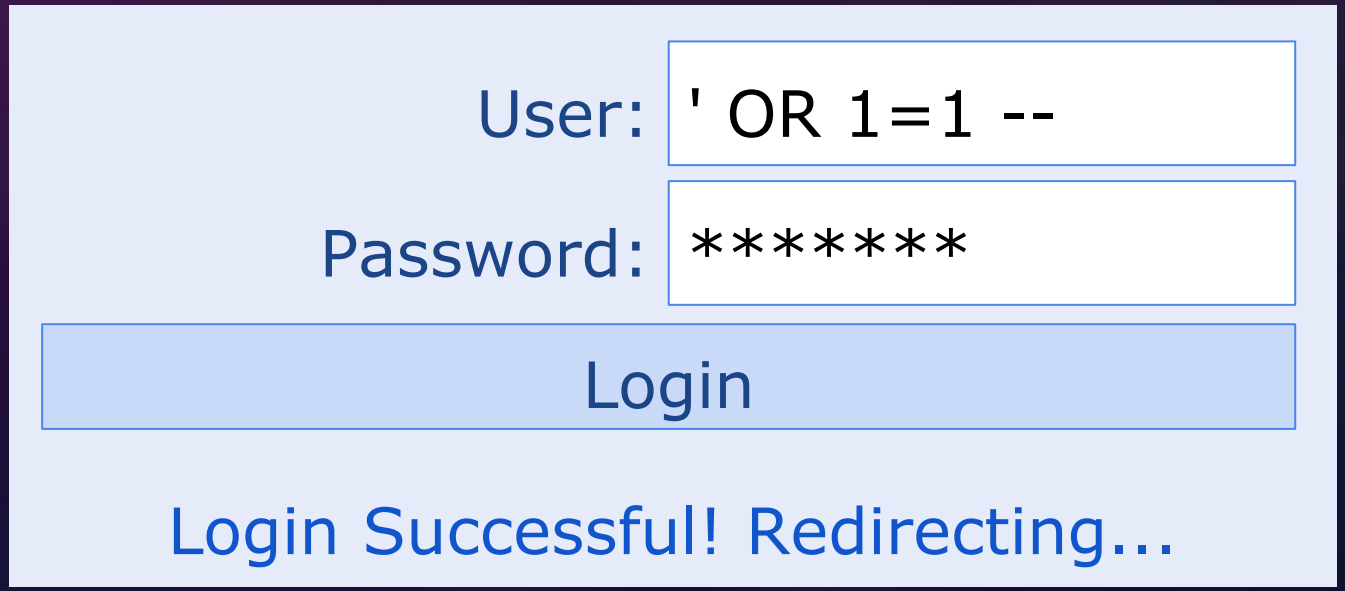
Prawo dot. "hakingu" w Polsce w 2007

Jeśli uzyskasz nieautoryzowany dostęp do informacji przełamując zabezpieczenie elektroniczne (lub innego rodzaju)

Możesz pójść do więzienia lub dostać grzywnę!

Była taka sprawa z SQL injection...

Była taka sprawa z SQL injection...



Była taka sprawa z SQL injection...

Story went like this:

1. The person reported the vulnerabilities to the company, and offered to fix them.

Była taka sprawa z SQL injection...

Story went like this:

1. The person reported the vulnerabilities to the company, and offered to fix them.

2. The company invited the person to sign the contracts & NDAs for the fix.

Była taka sprawa z SQL injection...

Historia szła tak:

1. Pewna osoba zgłosiła podatność SQLI pewnej firmie (i zapytała czy pomóc im naprawić)
2. Firma zaprosiła osobę na podpisanie NDA/umowy.
3. Po podpisaniu NDA osoba została aresztowana i postawiona przed sądem.

Prawo dot. "hakingu" w Polsce w 2007

Jeśli uzyskasz nieautoryzowany dostęp do informacji
przełamując zabezpieczenie elektroniczne (lub innego rodzaju)

Możesz pójść do więzienia lub dostać grzywnę!

Tyle, że w SQL injection...

```
SELECT * FROM users WHERE
username='thomas' AND password='47b65f2...'
```

nie ma ŻADNEGO
zabezpieczenia
(na tym polega problem)

Była taka sprawa z SQL injection...

Historia szła tak:

4. Osoba z historii została uniewinniona, ponieważ nie przełamała żadnych zabezpieczeń.

Ot taki szczegół.

(źródło: http://prawo.vagla.pl/node/8154)

Prawo dot. "hakingu" w Polsce obecnie

Jeśli znajdziesz podatność w systemie/sieci
ale ją od razu zgłosisz

To wszystko gra :)

(Przed wprowadzeniem w życie należy skonsultować się
z prawdziwym prawnikiem)

Podsumowanie

Podsumowanie

Podsumowanie

Podsumowanie

Podsumowanie

Ostatecznie wszystko rozbija się o szczegóły.

A każdy duży system informatyczny ma
bardzo bardzo dużo różnych szczegółów i szczegółików :)

Koniec

Czy są jakieś łatwe pytania?

Jeśli nie, to do zobaczenia około 16:00!

E-mail: gynvael@coldwind.pl Twitter: @gynvael YT: GynvaelEN

Blog: http://gynvael.coldwind.pl/ (Soon also: http://gynvael.live)

Additional slides follow

Either not finished or just extra

Encryption and Compression

Szczegóły na przykładach #3

What to recall from the Mumble Mumble part

- If something is properly encrypted,
  we cannot see the plaintext
- But we do know the packet sizes and timing

First compress, then encrypt

AAABAAACCCCCCCCAAA

First compress, then encrypt

AAABAAACCCCCCCCAAA

3A 1B 3A 7C 3A

First compress, then encrypt

AAABAAACCCCCCCCAAA

3A 1B 3A 7C 3A

¯_(ツ)_/¯

Wouldn't work the other way around

AAABAAACCCCCCCCAAA

J*KJNASF*)FK#FDH!(#$S

Wouldn't work the other way around

AAABAAACCCCCCCCAAA

J*KJNASF*)FK#FDH!(#$S

1J 1* 1K 1J 1N 1A 1S 1F 1* 1) 1F 1K 1# 1F 1D 1H 1! 1(1# 1$ S

Compression types: dictionary compression

RED AND GREEN ARE COLORS.
I LIKE GREEN MORE THAN I LIKE RED.
GREEN IS MUCH NICER.

82 characters

X AND Y ARE COLORS.
Z Y MORE THAN Z X.
Y IS MUCH NICER.
X:RED Y:GREEN Z:I LIKE

79 characters

Compression types: dictionary creation as you go

RED AND GREEN ARE COLORS.
I LIKE GREEN MORE THAN I LIKE RED.
GREEN IS MUCH NICER.

82 characters

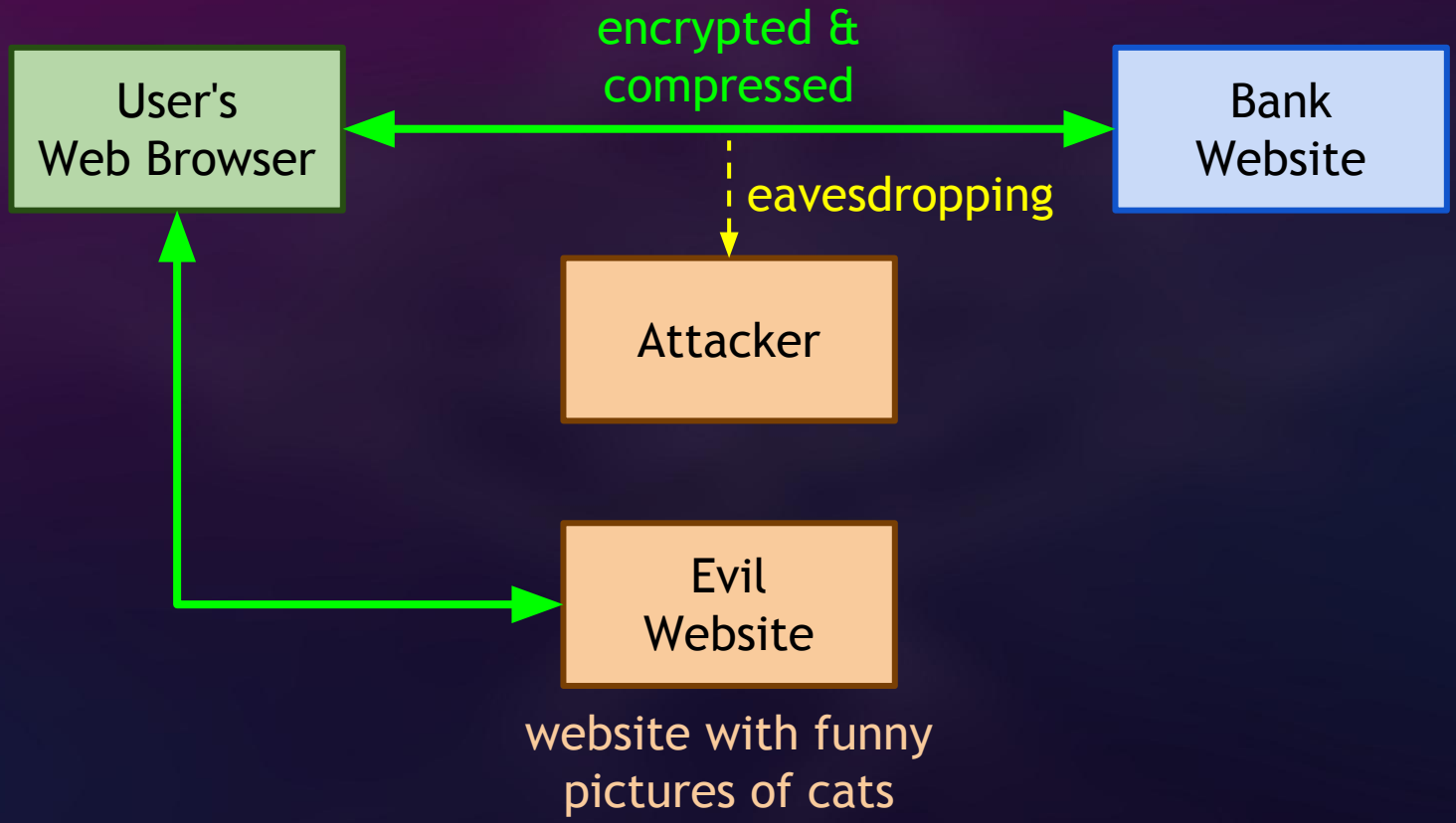
REDX AND GREENY ARE COLORS.
LIKEZ Y MORE THAN Z X.
Y IS MUCH NICER.

68 characters

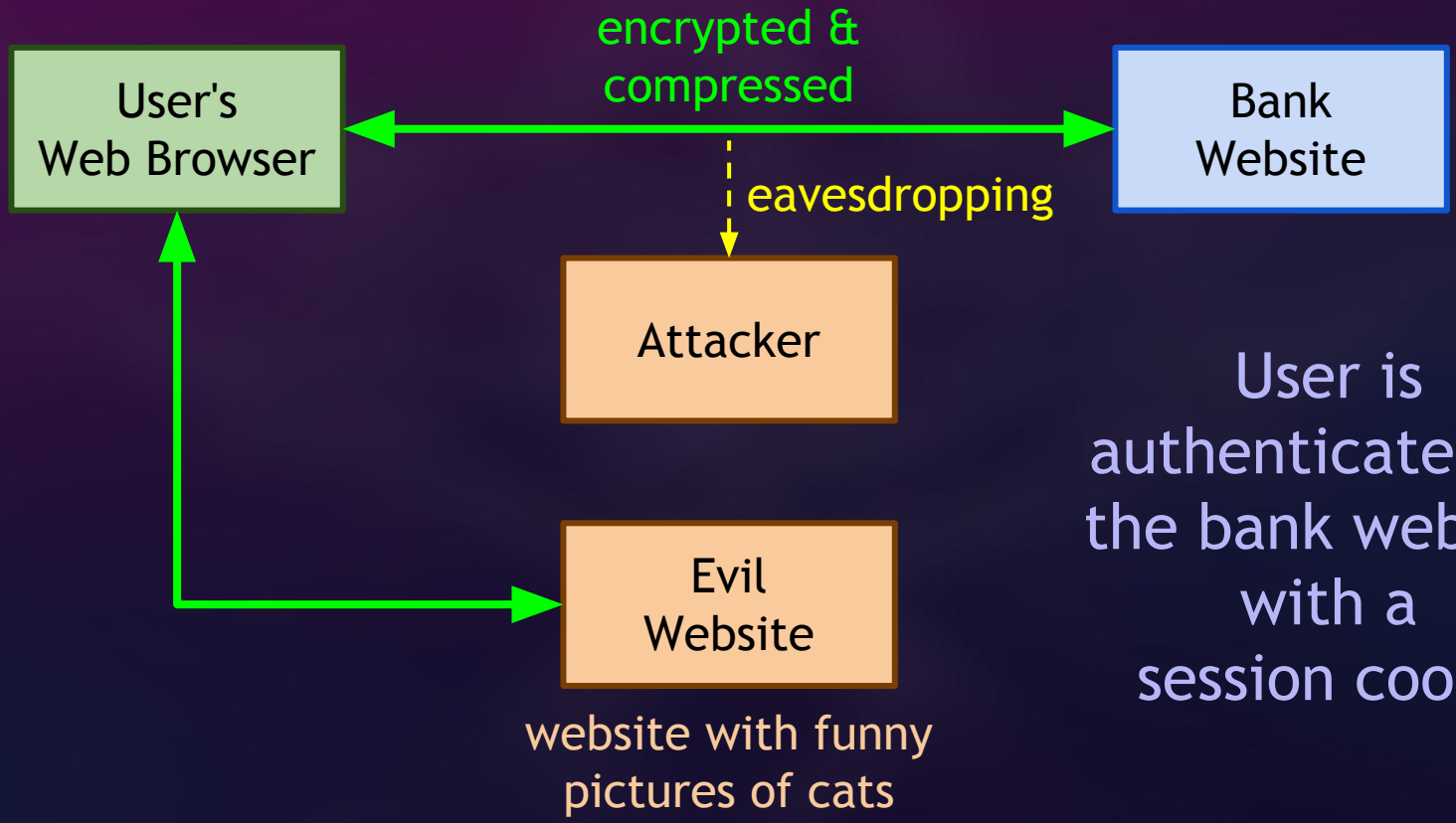
Here's a funny question

In modern Internet
can compression sabotage
encryption?

Typical scenario



Typical scenario



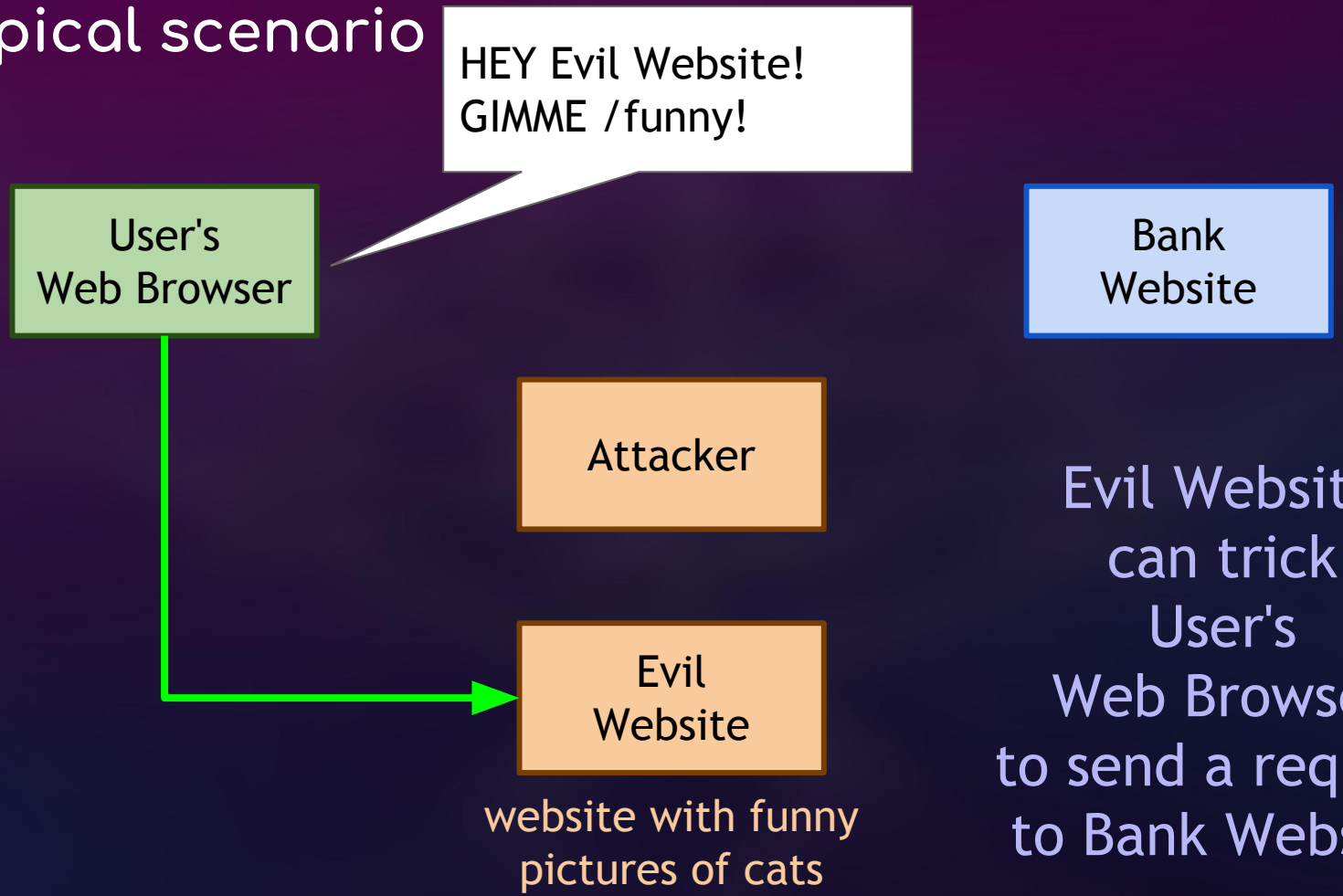
User is authenticated at the bank website with a session cookie

Typical scenario


```
GIMME /my_account.html
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h
```

(not a real HTTP REQUEST, but it's close enough)

Typical scenario

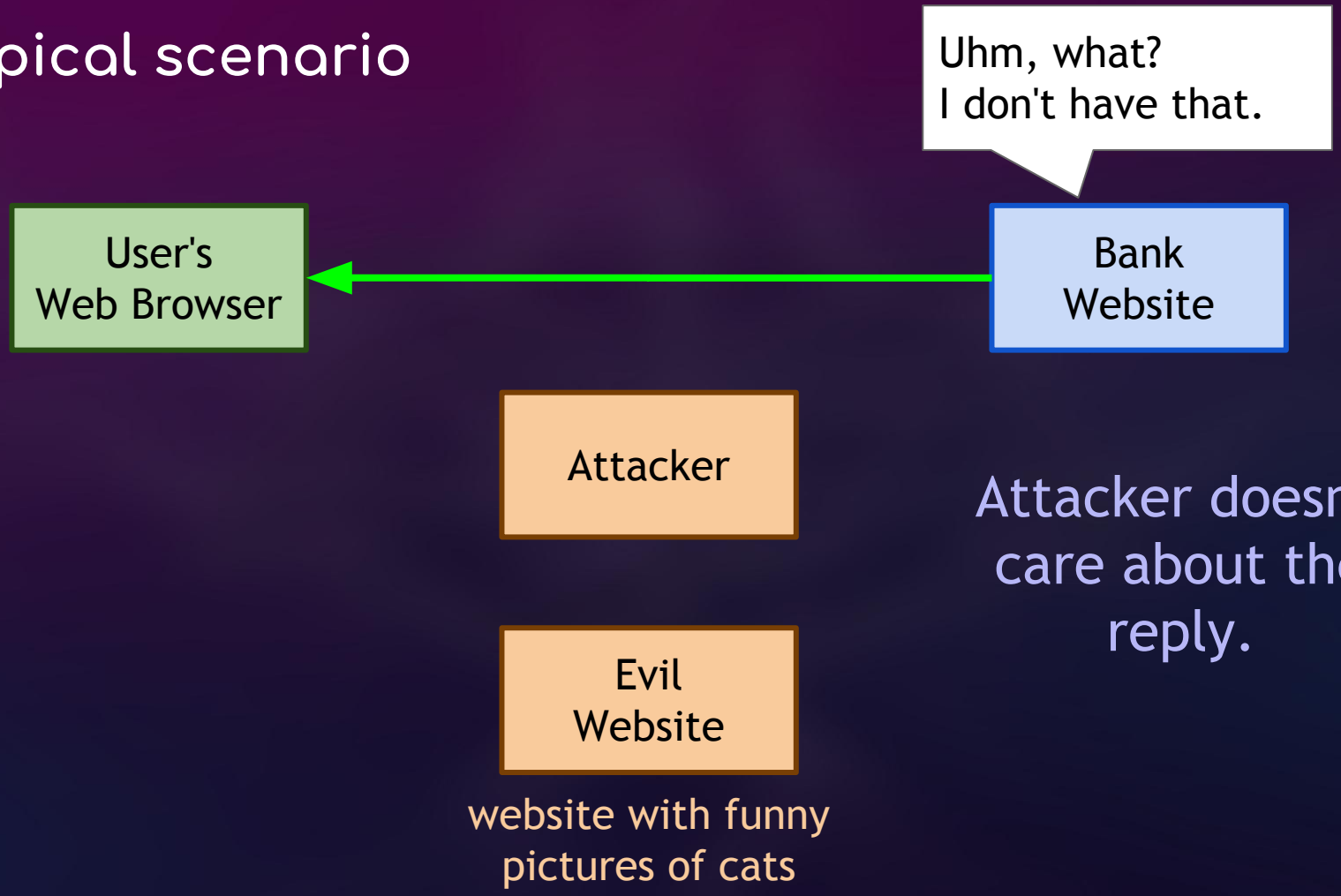


Typical scenario

Typical scenario

Remember:
Attacker can see only size of packet, not it's content!

Typical scenario



Attacker doesn't care about the reply.

Typical scenario

User's
Web Browser

Bank
Website

Attacker

Evil
Website

website with funny
pictures of cats

Attacker's goal:

somehow get the
session cookie

Compress → Encrypt

GIMME /cat.jpg
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

58 characters

GIMME /cat.jpg
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

58 characters

Attacker prepares the attack

GIMME /cat.jpg?MY SESSION COOKIE IS: a
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

82 characters

GIMME /cat.jpg?MY SESSION COOKIE IS: Xa
Xvn182fn1o3ajcas3881h

62 characters

Now attacker iterates over letters

GIMME /cat.jpg?MY SESSION COOKIE IS: b
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

82 characters

GIMME /cat.jpg?MY SESSION COOKIE IS: Xb
Xvn182fn1o3ajcas3881h

62 characters

Now attacker iterates over letters

GIMME /cat.jpg?MY SESSION COOKIE IS: c
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

82 characters

GIMME /cat.jpg?MY SESSION COOKIE IS: Xc
Xvn182fn1o3ajcas3881h

62 characters

Fast forward

GIMME /cat.jpg?MY SESSION COOKIE IS: u
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

82 characters

GIMME /cat.jpg?MY SESSION COOKIE IS: Xu
Xvn182fn1o3ajcas3881h

62 characters

And hit! We get 'v'

GIMME /cat.jpg?MY SESSION COOKIE IS: v
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

82 characters

GIMME /cat.jpg?MY SESSION COOKIE IS: vX
Xn182fn1o3ajcas3881h

61 characters

Continue with next letter

GIMME /cat.jpg?MY SESSION COOKIE IS: va
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

83 characters

GIMME /cat.jpg?MY SESSION COOKIE IS: vXa
Xn182fn1o3ajcas3881h

62 characters

Continue with next letter until you hit it...

GIMME /cat.jpg?MY SESSION COOKIE IS: vn
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

83 characters

GIMME /cat.jpg?MY SESSION COOKIE IS: vnX
X182fn1o3ajcas3881h

61 characters

And the next...

GIMME /cat.jpg?MY SESSION COOKIE IS: vn1
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

84 characters

GIMME /cat.jpg?MY SESSION COOKIE IS: vn1X
X82fn1o3ajcas3881h

61 characters

And the next...

GIMME /cat.jpg?MY SESSION COOKIE IS: vn18
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

85 characters

GIMME /cat.jpg?MY SESSION COOKIE IS: vn18X
X2fn1o3ajcas3881h

61 characters

Until you get everything

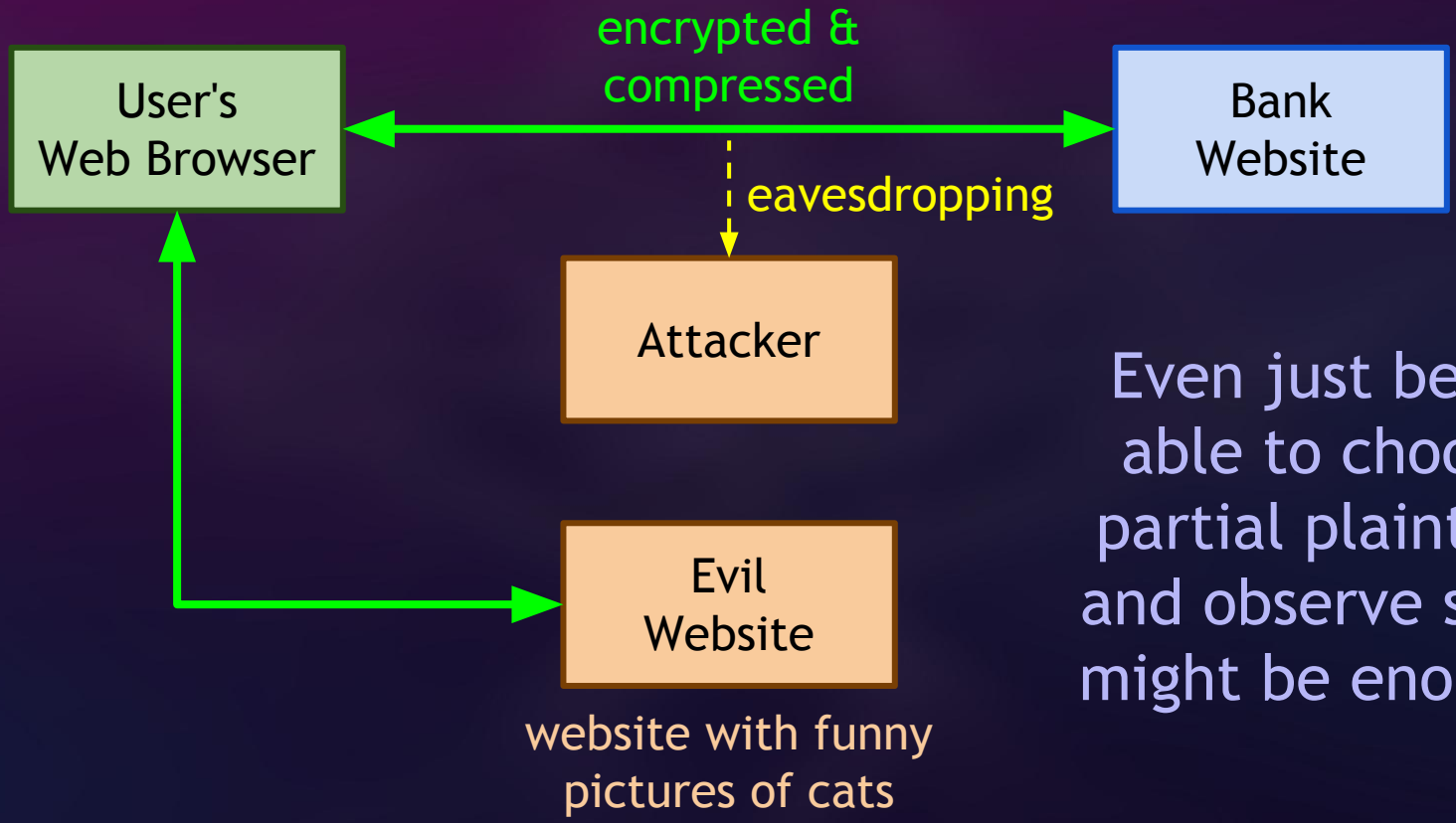
GIMME /cat.jpg?MY SESSION COOKIE IS: vn182fn1o3ajcas3881h
MY SESSION COOKIE IS: vn182fn1o3ajcas3881h

101 characters

GIMME /cat.jpg?MY SESSION COOKIE IS: vn182fn1o3ajcas3881hX
X

61 characters

Typical scenario



Even just being able to choose partial plaintext and observe sizes might be enough!

For details see

"Compression and Information Leakage of Plaintext"

John Kelsey

1 Introduction

Cryptosystems like AES and triple-DES are designed to encrypt a sequence of input bytes (the plaintext) into a sequence of output bytes (the ciphertext) in such a way that the output carries no information about that plaintext except its length. In recent years, concerns have been raised about "side-channel" attacks on various cryptosystems–attacks that make use of some kind of leaked information about the cryptographic operations (e.g., power consumption or timing) to defeat them. In this paper, we describe a somewhat different kind of side-channel provided by data compression algorithms, yielding information about their inputs by the size of their outputs. The existence of some information about a compressor's input in the size of its output is obvious; here, we discuss ways to use this apparently very small leak of information in surprisingly powerful ways.

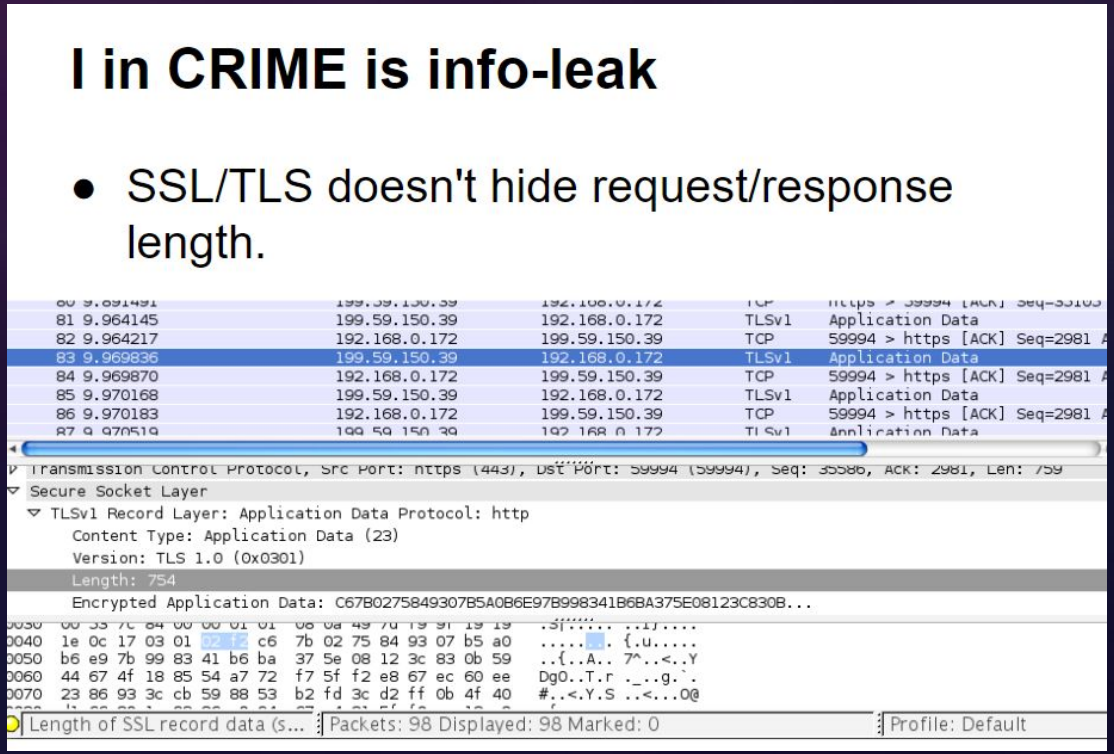
The compression side-channel differs from side-channels described in [Koc96] [KSHW00] [KJY00] in two important ways:

1. It reveals information about plaintext, rather than key material.
2. It is a property of the *algorithm*, not the implementation. That is, any implementation of the compression algorithm will be equally vulnerable.

And for actual HTTPS attacks see

"The CRIME attack"

Juliano Rizzo and Thai Duong



Protip

Crypto is hard.
No, really.

Do not implement and roll out your own crypto unless you reaaaaaally know what you're doing.

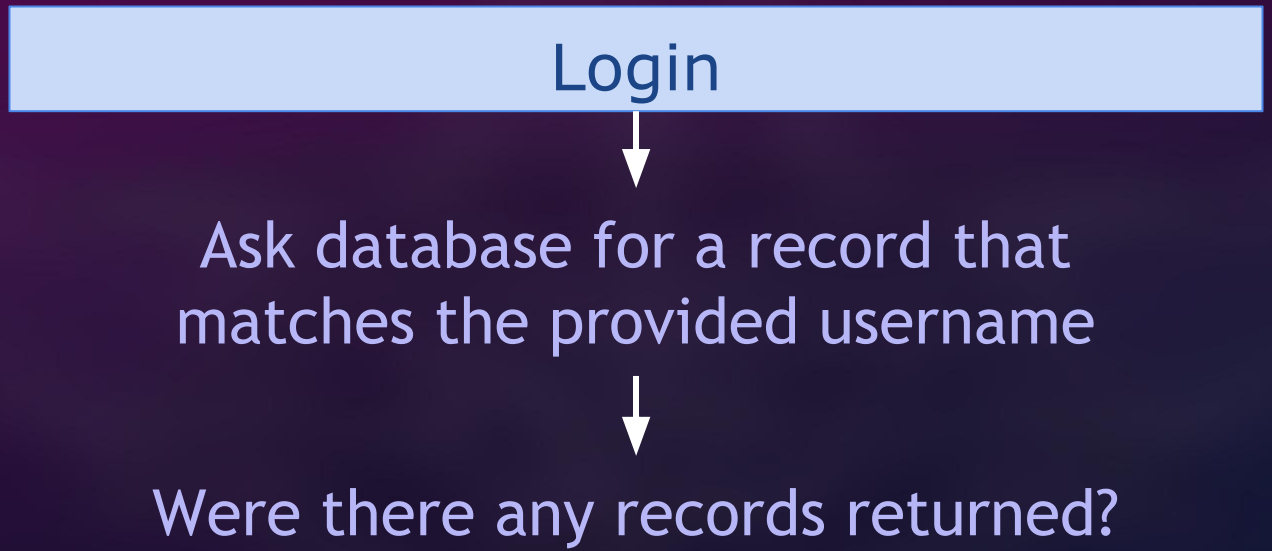
Compression and encryption summary

- Applied crypto is fun!
- It's all about the tiny details!

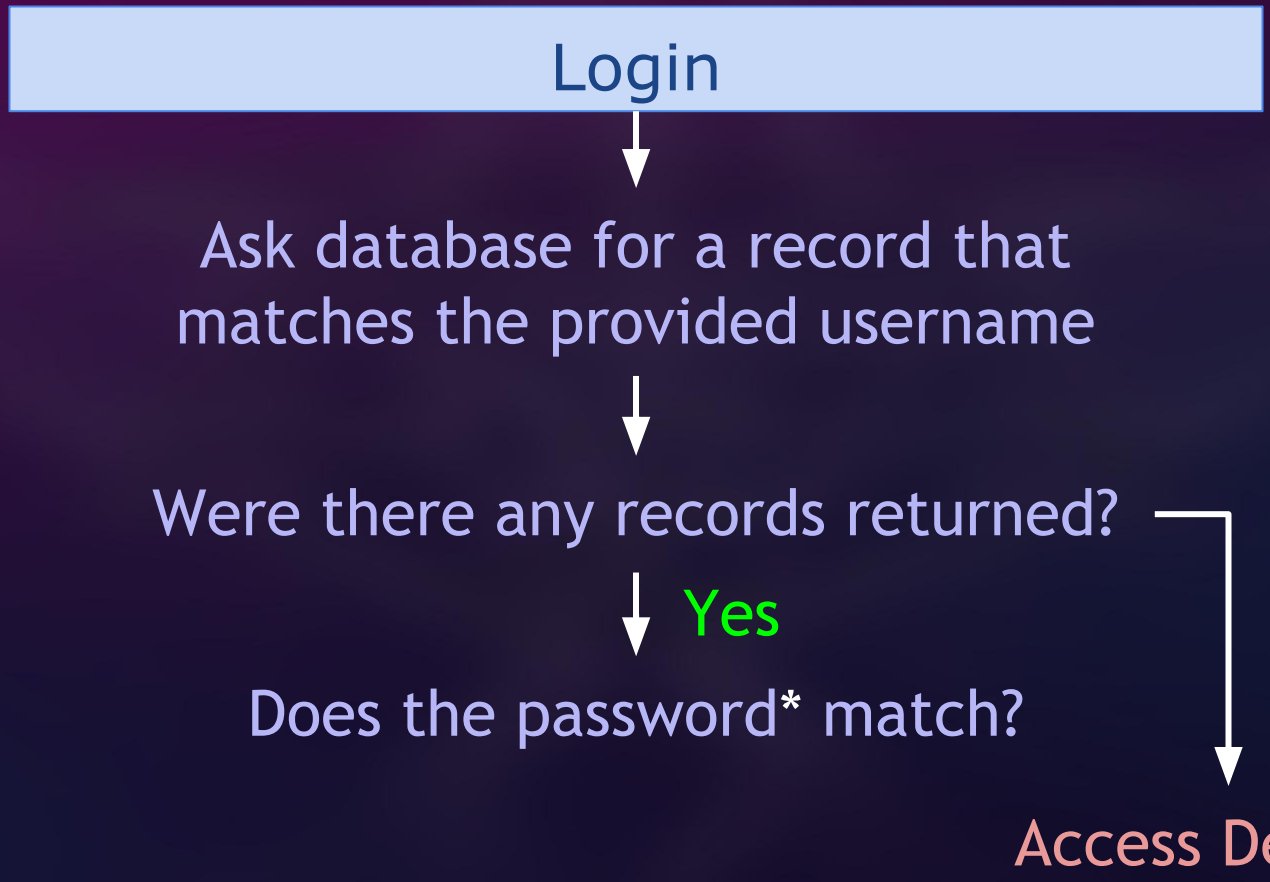
Simple authentication (1)

Simple authentication (1)

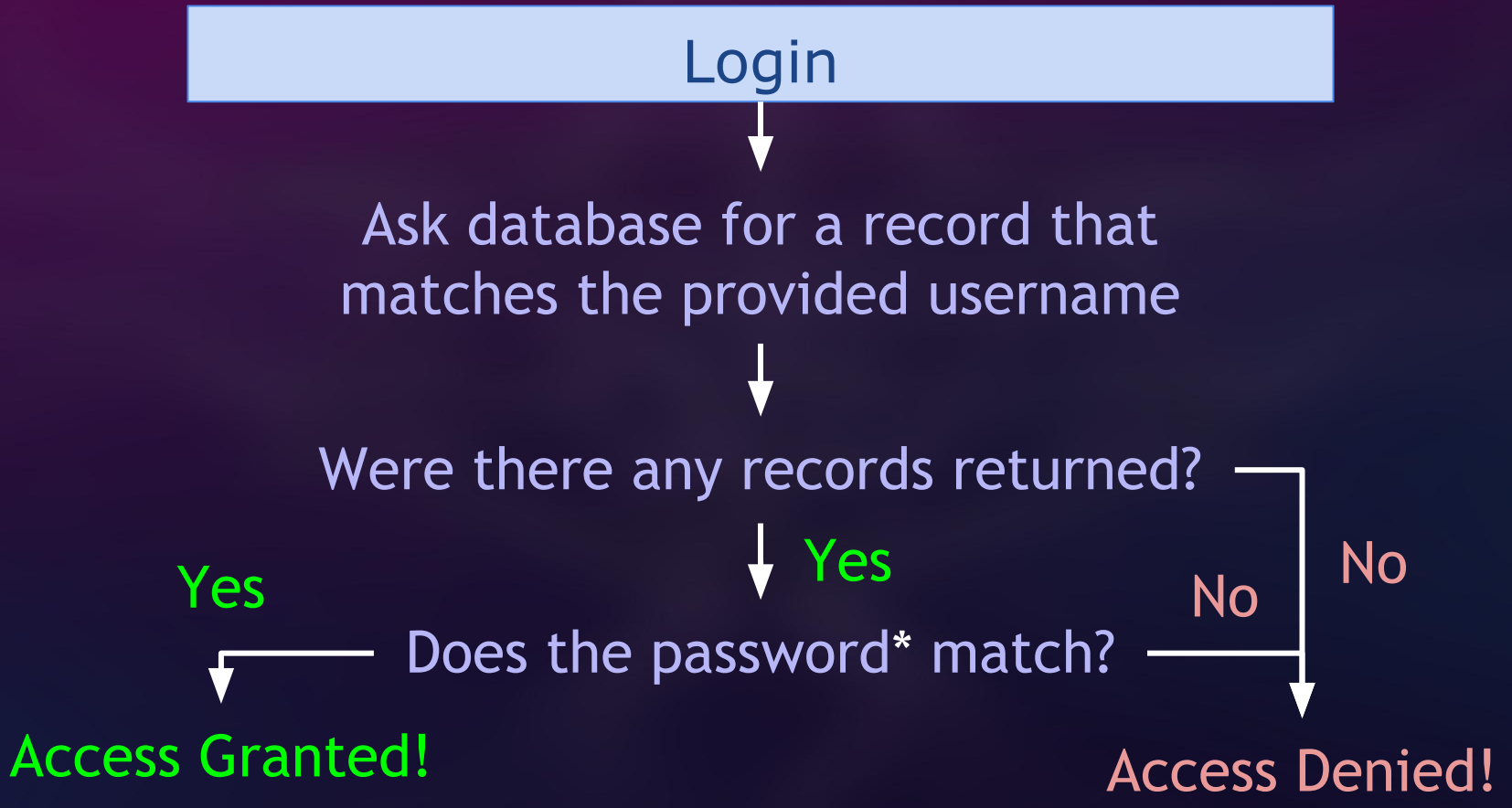
Simple authentication (1)



Simple authentication (1)

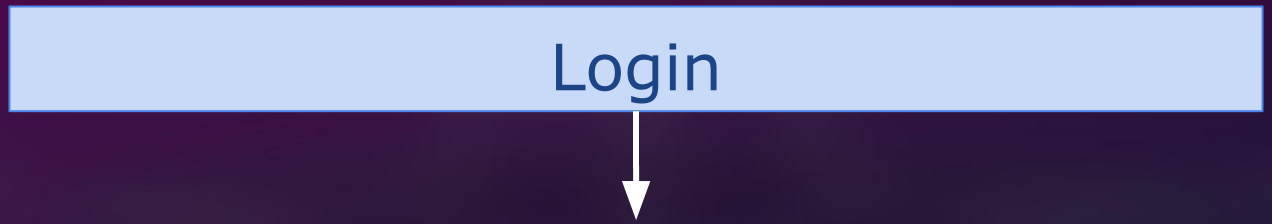


Simple authentication (1)



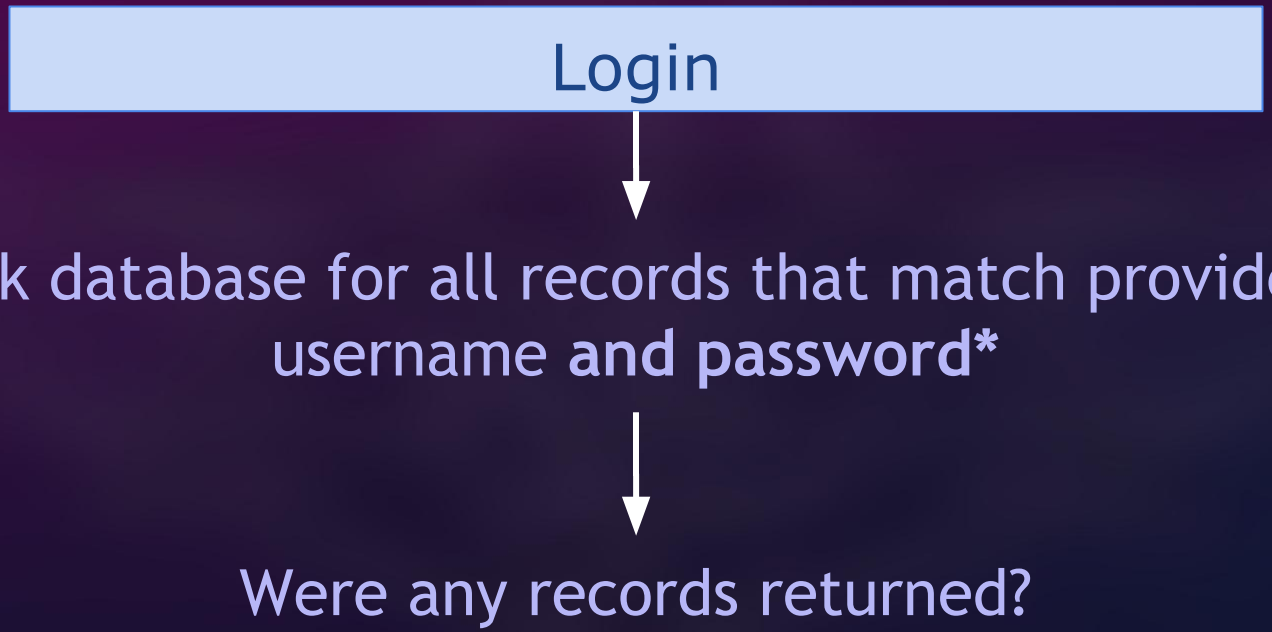
Simple authentication (2)

Simple authentication (2)

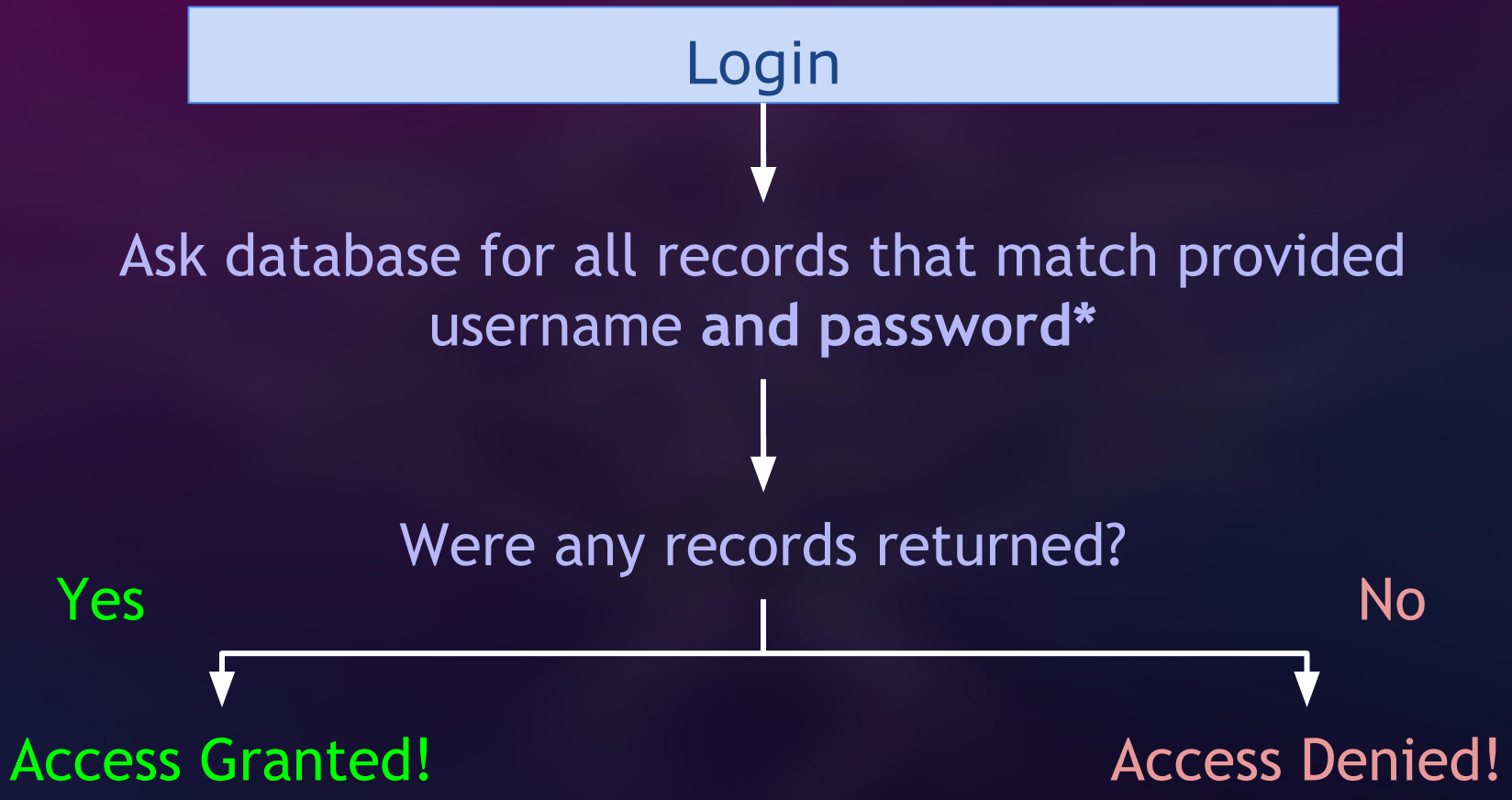


Ask database for all records that match provided username **and password***

Simple authentication (2)



Simple authentication (2)



A little bit of history - old-style databases

APPLICATION

Give all records plz!

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

A little bit of history - old-style databases

APPLICATION

ID	Username	Password*
0	admin	

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

A little bit of history - old-style databases

APPLICATION

ID	Username	Password*
0	admin	87bd4c819a...
1		

downloading takes time

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

A little bit of history - old-style databases

APPLICATION

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...

downloading takes time

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

A little bit of history - old-style databases

APPLICATION

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	

downloading takes time

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

A little bit of history - old-style databases

APPLICATION

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

A little bit of history - old-style databases

APPLICATION

Filtering...
(username must be thomas)

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

A little bit of history - old-style databases

APPLICATION

Filtering...
(username must be thomas)

ID	Username	Password*
1	thomas	47b65f2ac9...

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

A little bit of history - old-style databases

APPLICATION

Processing...

ID	Username	Password*
1	thomas	47b65f2ac9...

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

A little bit of history - old-style databases

APPLICATION

Processing...

ID	Username	Password*
1	thomas	47b65f2ac9...

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

A little bit of history - old-style databases

APPLICATION

Processing...

ID	Username	Password*
1	thomas	47b65f2ac9...

OK! Password match!

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

Maybe the database could do the filtering...

APPLICATION

But how to tell the database how to filter?

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

Maybe the database could do the filtering...

APPLICATION

SQL
a specialized "query" language

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

Maybe the database could do the filtering...

APPLICATION

```
SELECT *
FROM users
WHERE
username='thomas'
AND
password='47b65f2...'
```

give me all records that match username and password

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

Maybe the database could do the filtering...

APPLICATION

Filtering (and some processing) is now done on the database server

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

Maybe the database could do the filtering...

APPLICATION

ID	Username	Password*
1	thomas	47b65f2ac9...

less records
faster
download

REMOTE DATABASE SERVER

ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

Maybe the database could do the filtering...

APPLICATION

Processing...

ID	Username	Password*
1	thomas	47b65f2ac9...

OK! We got a record!

REMOTE DATABASE SERVER

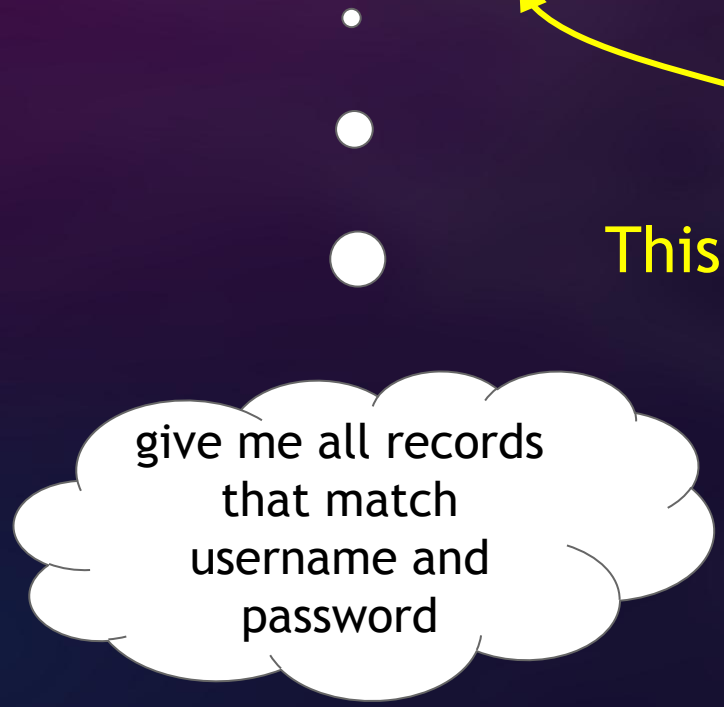
ID	Username	Password*
0	admin	87bd4c819a...
1	thomas	47b65f2ac9...
2	marta	cfa954fd82...

Protip

Be very very careful when dealing with user-controlled data and any non-trivial query languages!

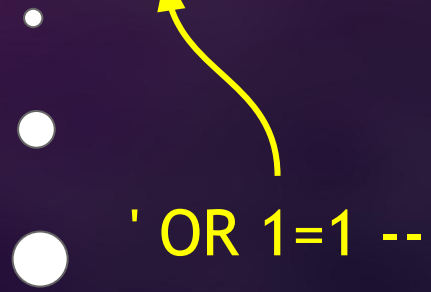
SQL Injection

```
SELECT * FROM users WHERE
username='thomas' AND password='47b65f2...'
```



SQL Injection - sometimes you can do this...

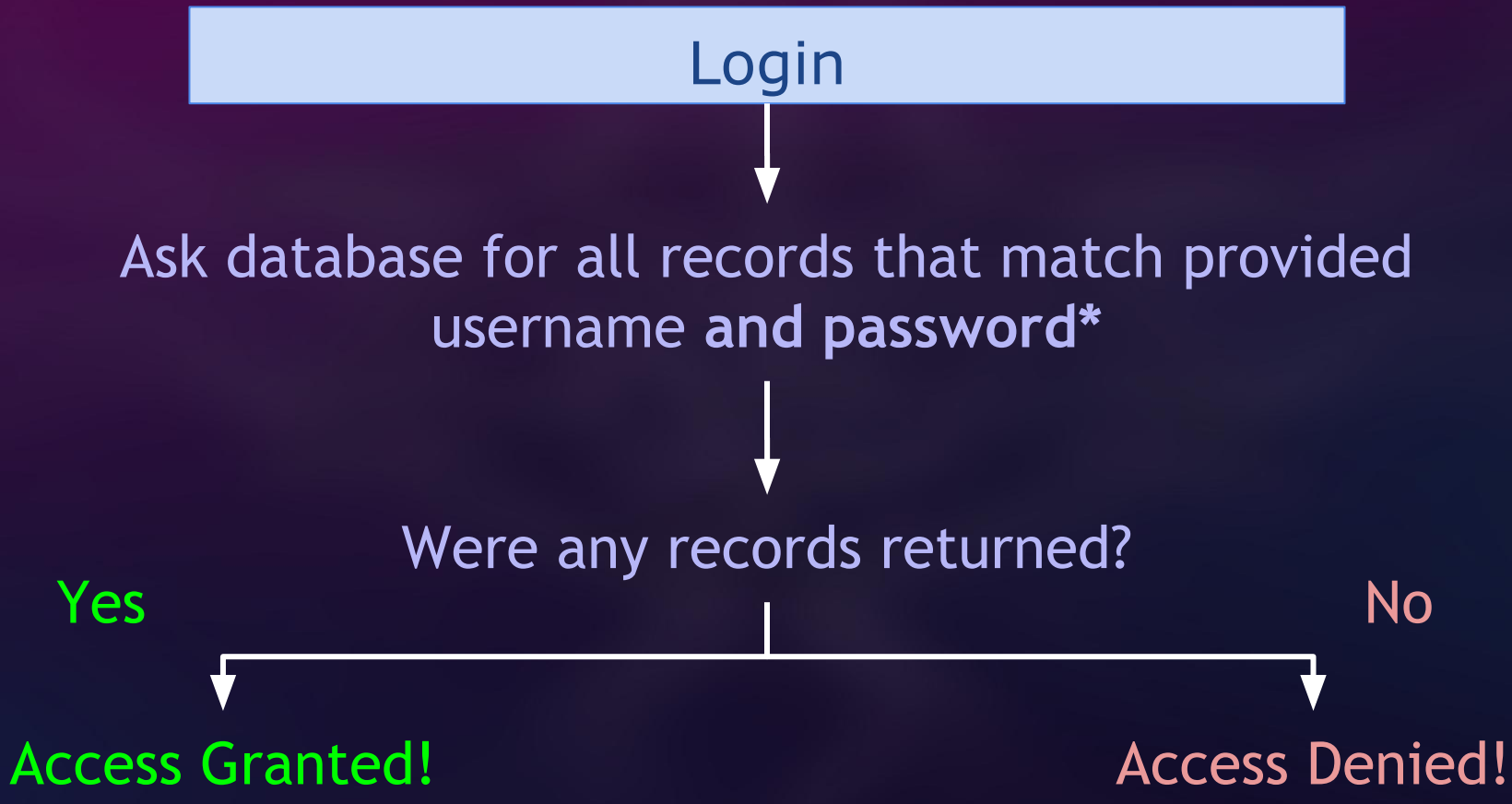
```
SELECT * FROM users WHERE
username='' OR 1=1 -- ' AND password='47b65f2...'
```



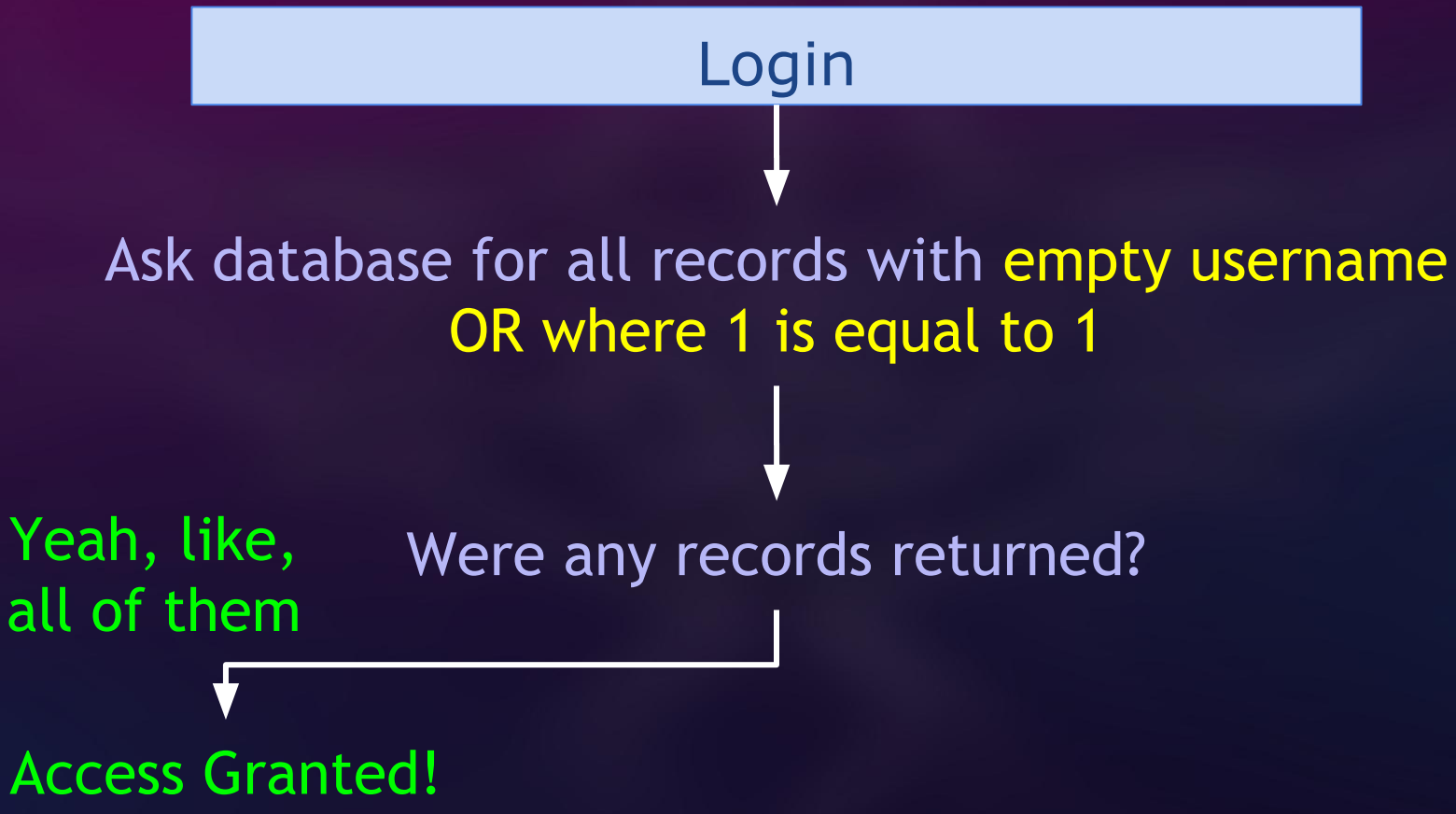
This is now just a comment

give me all records
with empty username
OR
where 1 is equal to 1

Simple authentication (2) - as intended

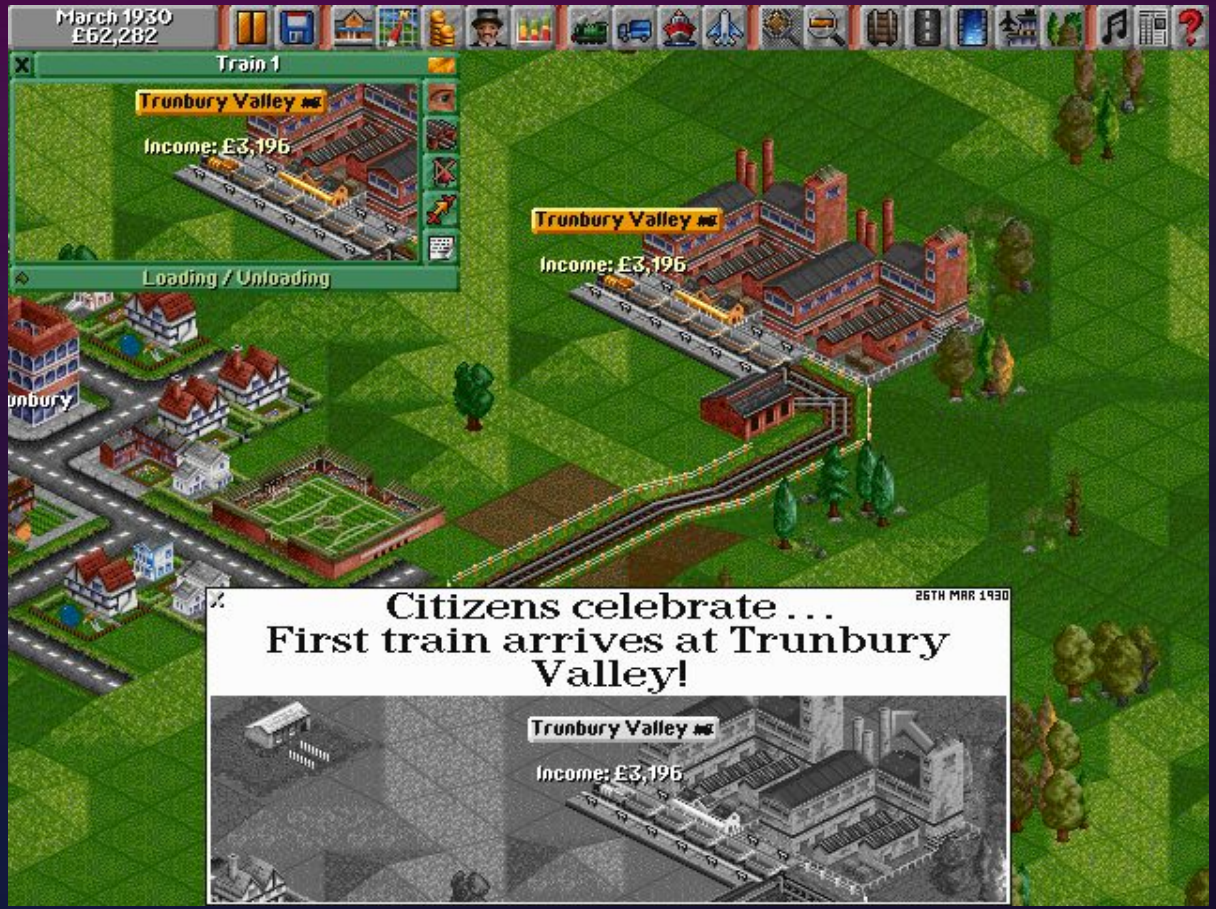


Simple authentication (2) - after SQL injection



Transport Tycoon (1994, MicroProse)

How the game worked



The player build train, road, ship and plane connections between points to earn money.

Building infrastructure & buying vehicles costed money.

Here's the thing about 32-bit signed integers

Range (circa):

-2 billion ⟶ +2 billion

And all hell breaks loose if you try to operate on bigger numbers ;)

Here's the thing about 32-bit signed integers

Here's a puzzle:

Transport Tycoon (1994, MicroProse)

That nasty physics

Details in examples #4