

# Picviz

Sébastien Tricaud

INL  
15 rue Berlier  
75013 Paris, France

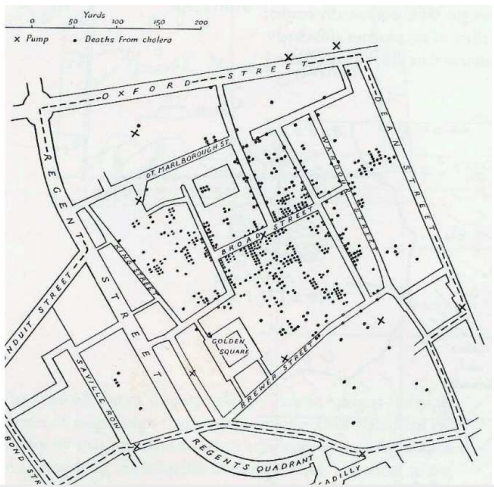
Hack.lu lighting talk, Luxembourg 2008



# Body check

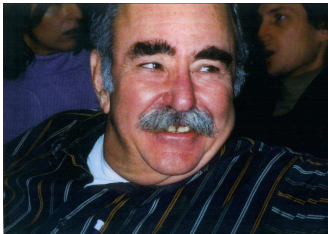


# Cholera epidemic in London



## Inventor

Invented and especially applied in 1959 by Alfred Inselberg. Senior Fellow San Diego Supercomputing Center and Computer Science and Applied Mathematics Departments Tel Aviv University, Israel

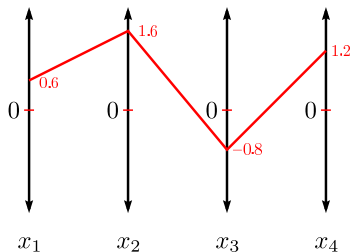


- Conflict Resolution, One-Shot Problem and Air Traffic Control, 1st Canadian Conf. on Comp. Geom., 1989, 26-9



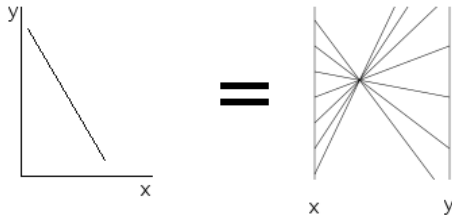
## What are parallel coordinates ?

$$\vec{u} = (0.6, 1.6, -0.8, 1.2) \in \mathbb{R}^4$$



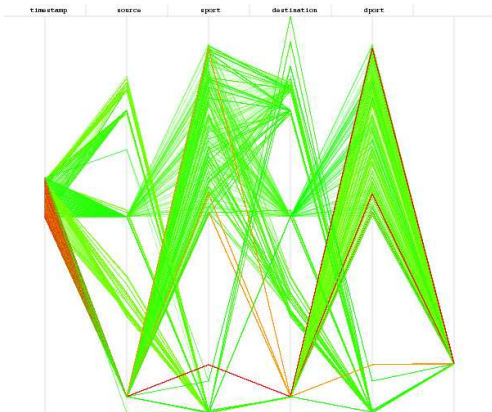


## Line correlation





## Finding OpenVPN traffic



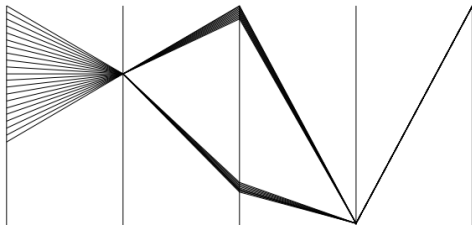


## All you can chick

- N dimensions,  $\infty$  of events, any kind of event
- Every axis
  - is a different variable
  - should be equidistant
  - receives the minimal value of each variable at the bottom, and maximum at the top
- The order matters
  - Time = first axis
  - Source on the left, Destination on the right
  - Garbage data on the last axis

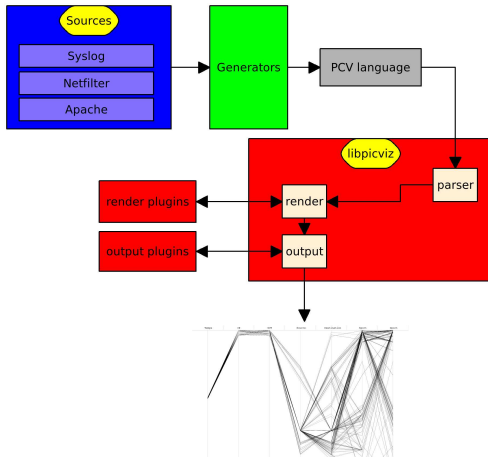


# Picviz





# Architecture





## Goal

- Allow creation and exploitation of parallel coordinates
  - Easy to script
  - Easy to understand (after some training ;))
  - Easy to filter
  - Magical when one want to understand millions of events



## Tools

Picviz provides:

- **Perl scripts:** Parse logs to create PCV
- **pcv:** Binary transforming PCV into image
- **picviz-gui:** Graphical UI to dig into lines

## Using

### PCV source

```
header { title = "Hacklu"; }  
axes {  
    timeline t;  
    integer in;  
}  
data {  
    t="14:42", in="12" [color="red"];  
    t="14:45", in="432";  
}
```

### Generate the image

```
pcv -Ttplplot fichier.pcv 'filter'
```



## Filterer

- Filtering points: show plot  $> 250$  on axis 2
- Filtering points: show plot  $> 50\%$  on axis 2
- Filtering strings: hide value = `".*[F]oo.*"` on axis 1



## Axes types

- Time: timeline, years
- Numbers: integer, short, gold, char
- Addresses: ipv4, ipv6
- Strings: string

## Time matters

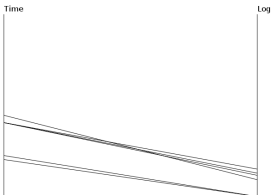
- Scale the variable
- a 24h representation:
  - Allows to see what time events occur
  - Prevent you from differentiate days
- By showing my logs during lectures, people know when I go sleep :-D





## String position

Basic algorithm:



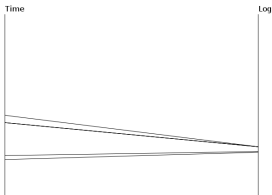
### Logs

```
ab
ba
invalid user carlabru
invalid user blingbling
invalid user admin
invalid user root
```



## String position

Prefix algorithm:

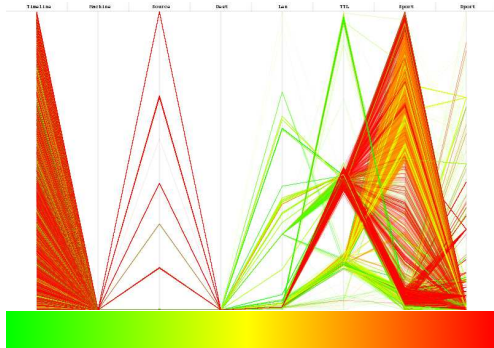


### Logs

```
ab
ba
invalid user carlabru
invalid user blingbling
invalid user admin
invalid user root
```

# Heatlines

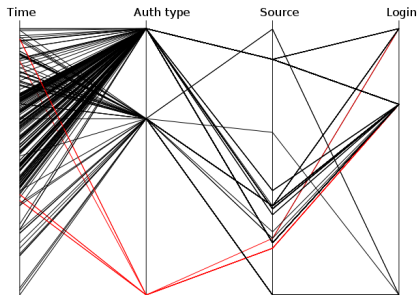
The more the line is drawn, the more red it gets



## Picviz::Dshield

```
use Picviz :: Dshield;  
$dshield = Picviz :: Dshield->new();  
  
if ($dshield->ip_check("192.168.1.42")) {  
    print "IP_found";  
} else {  
    print "IP_not_found";  
}
```

# SSH authentication





## Artcor.pl

- Simple script written from looking at PC images
- Alert if:
  - IP and port matches Dshield database
  - Same login authentications from multiple IP addresses
  - Several authentication methods used



## Questions ?

Picviz

<http://www.wallinfire.net/picviz>

Slides: <http://www.wallinfire.net/files/picviz-hacklu2008.pdf>