Securing cities with CCTVs?

Not so sure - A urban guerrilla perspective

Eric Filiol & **Thibaut Scherrer** (speaker)

ESIEA
Operational Cryptology and Virology Laboratory $(C+V)^O$

June 22^{nd}, 2013

Agenda

Agenda

Introduction

- CCTVs have nowadays invaded our cities.
  - One CCTV camera for every 32 people in UK (The Guardian, March 2^{nd}, 2011).
- Presented by politicians as the KEY technology to answer urban security issues.
- In fact, can also be dedicated to citizens' mass surveillance. Data are processed by private companies.
- `http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance`
- `http://owni.fr/2011/12/15/le-palmares-des-villes-sous-surveillance/`

Introduction (2)

- Do CCTVs really provide security?
  - Equivalently (attacker's perspective), can CCTV be bypassed easily or not?
- In a more wider context (urban guerilla), could Police forces and armies really rely on CCTV network to protect citizens efficiently.
  - Equivalently (attacker's perspective), is is possible to blind one-eyed police and states?
- Critical issues in Europe increasing context of riots and revolution 2.0.
- Alternative issues: is it possible for attackers to access military-like technology for a few euros (e.g. infra-red cameras).

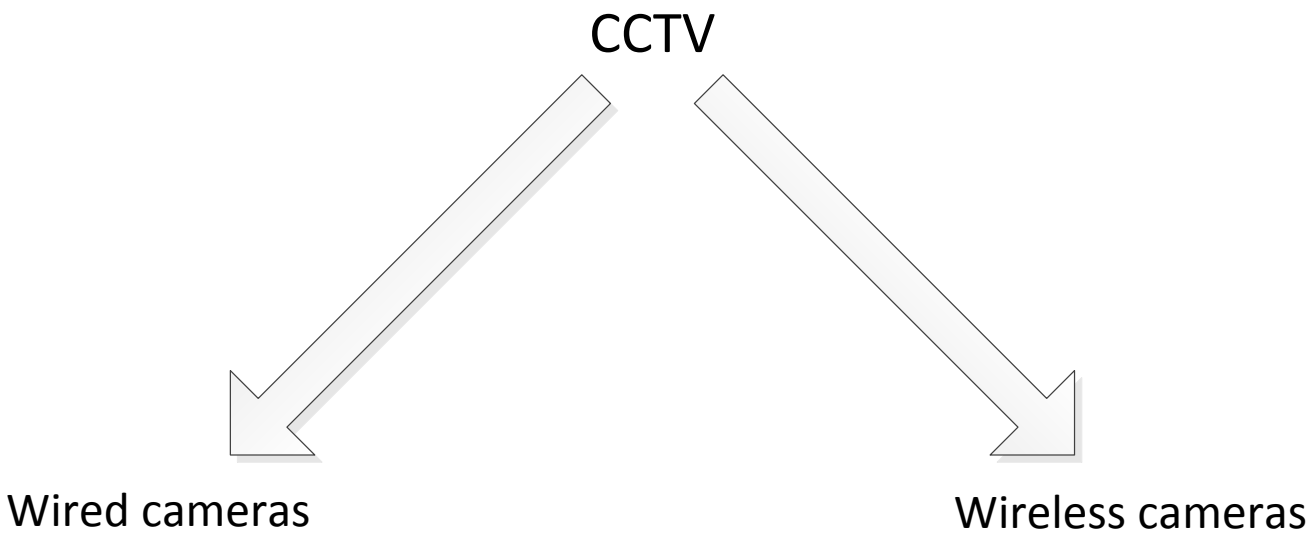
Agenda

CCTV

CCTV (Close Circuit TeleVision)

System of cameras set up in public or private areas in order to monitor them.

Techniques: connecting CCTVs



Two main categories

Techniques: orientation modes

Pan, Tilt, Zoom (hemispheric)

Fixed camera (focused/oriented)

Techniques: Color vs. B/W

Color

Grayscale

- Color: better rendering/details, enables color-based identification (blue police car different from red bad guy ferrari).
- B&W: cheaper and much light-sensitive (better resolution in under-lit areas).

Technologies: CCD sensors

Charge Coupled Device: pros and cons

+ High resolution
+ Little noise level
+ Color rendering
- Blooming and smearing sensitive
- Not enough dynamism in cases of highly contrasted pictures

Technologies: CCD issues

Blooming effect

Smearing effect

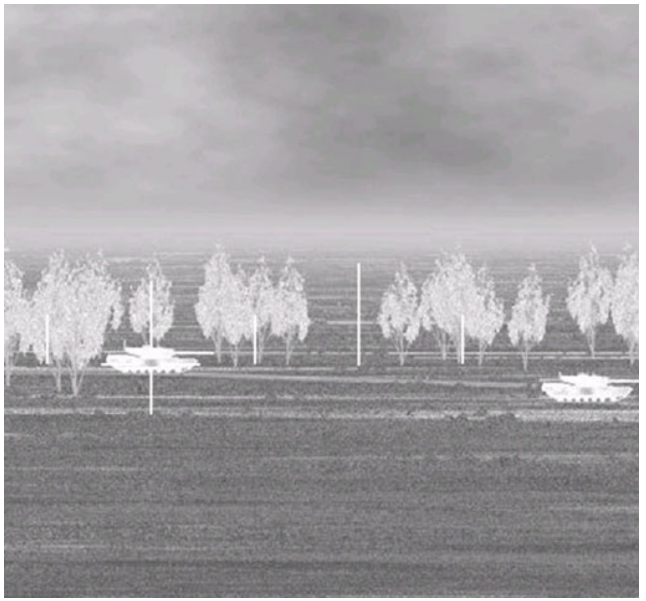
Technologies: CMOS sensors

Complementary Metal Oxyde Semiconductor: pros and cons

+ Good dynamic behaviour in contrasted situations
+ High picture frequency
+ Region Of Interest functionality
+ Low power consumption
- Poor sensitivity in under-lit situations

Technologies: night vision

Infrared imagery



Thermal imagery

Light intensification

Agenda

Introduction: what are attackers' main issues

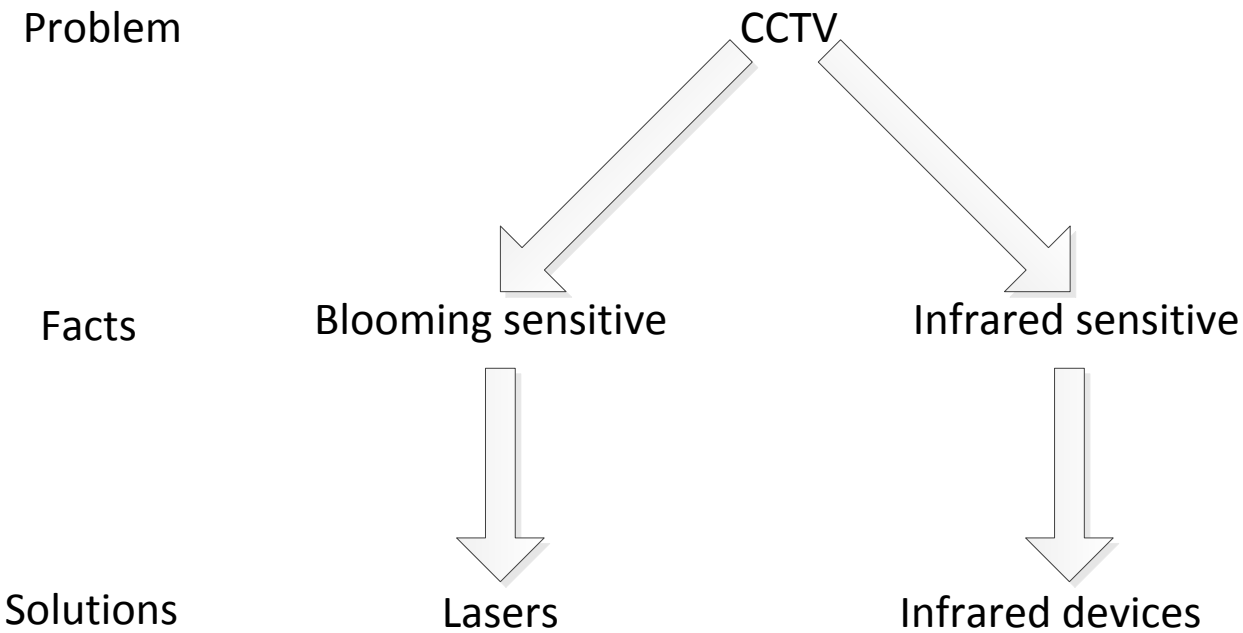
$$\left.\begin{array}{r} \neq \text{ techniques} \\ \neq \text{ technologies} \end{array}\right\} \Rightarrow \neq \text{ solutions to tackle with CCTVs}$$

- Lame issues not covered here: painting CCTVs (what about CCTVs that you cannot see, CCTVs out of reach...).
- How to manage a large set of CCTVs simultaneously to make a whole area blind (urban guerilla issue)?

Introduction: easy case to solve (WiFi CCTVs)

Why spending time to design complex electronic devices when jamming signal is enough?

The Way of the Warrior



Strategies and angles of attack

Agenda

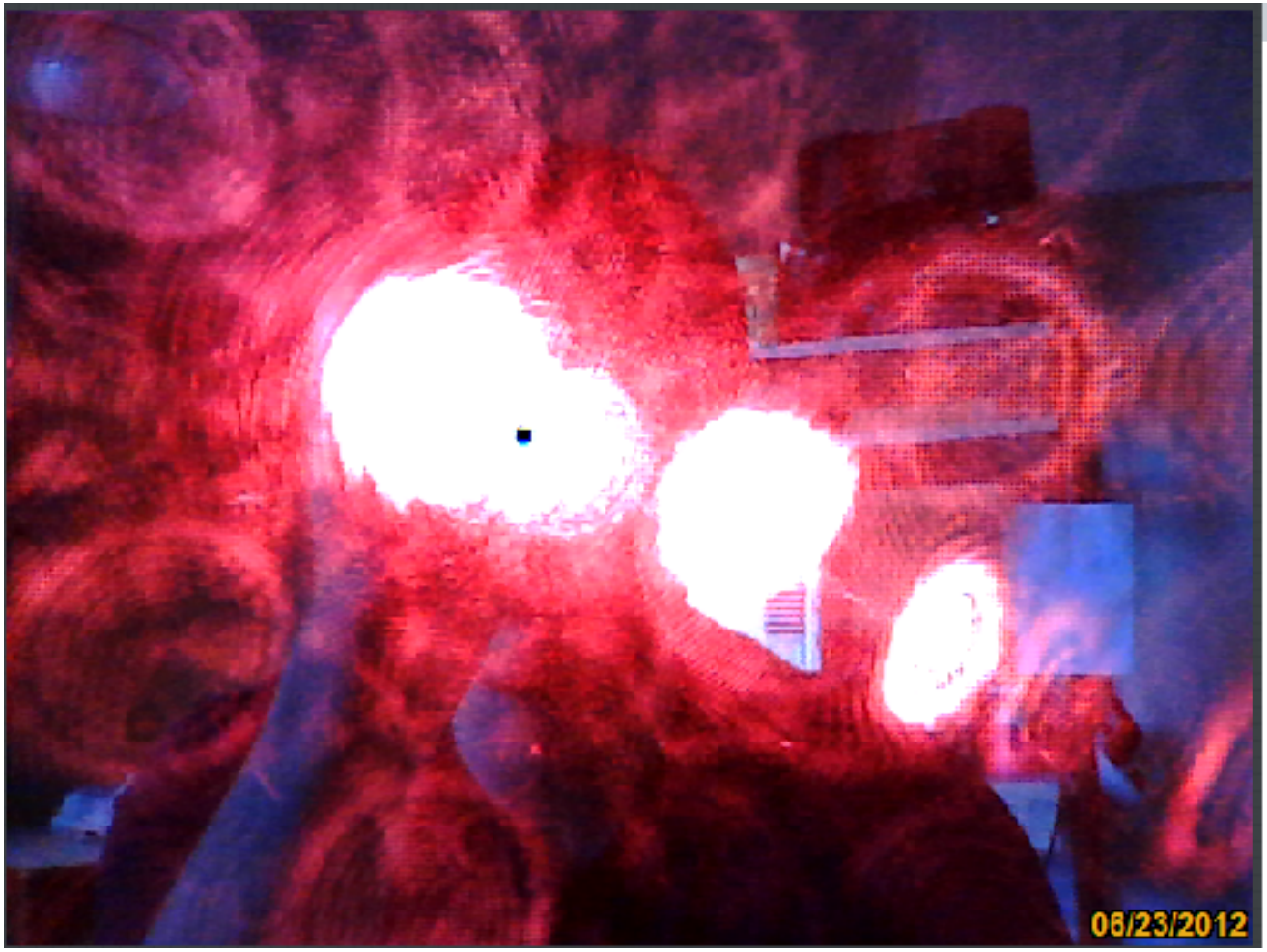
How to: Lasers

Blooming CCTVs with lasers

One of the lasers we have tested

How-to: lasers (2)

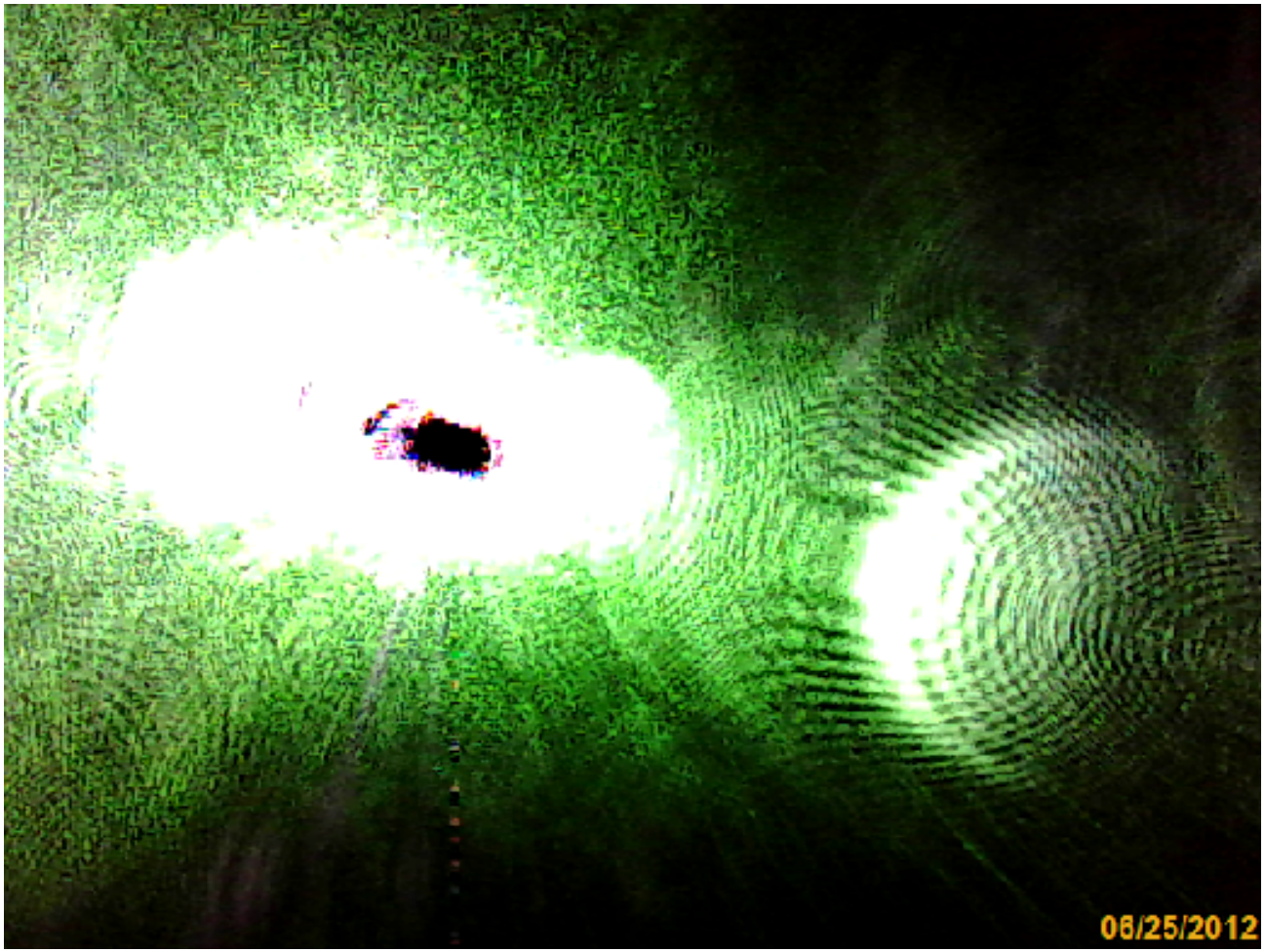
Blooming CCTVs with lasers



Blooming camera with a less than 1mW laser

How-to: lasers (3)

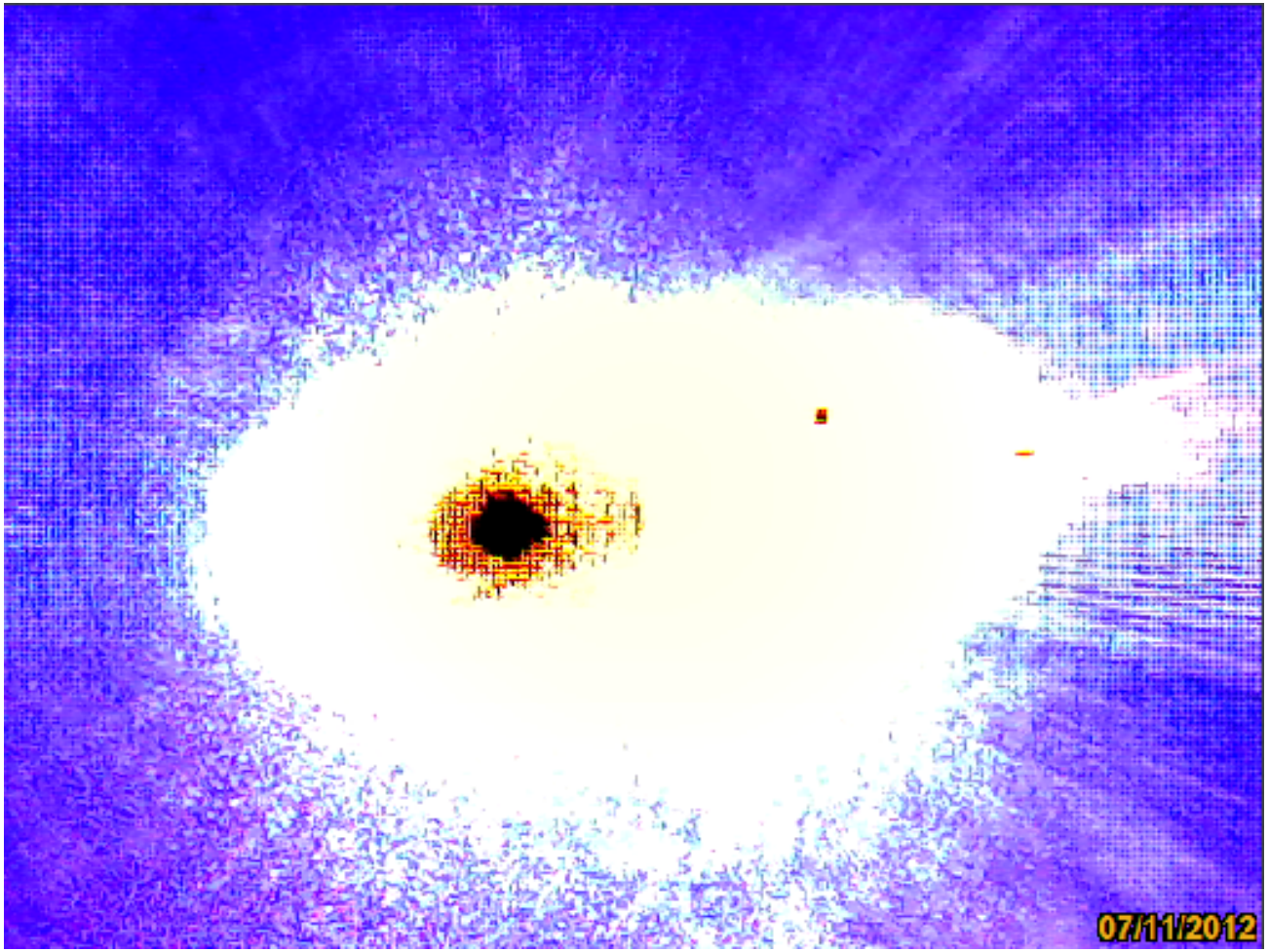
Blooming CCTVs with lasers



Blooming camera with a 25mW laser

How-to: lasers (4)

Blooming CCTVs with lasers



Blooming camera with a 200mW laser

How-to: lasers (5)

Targeting the camera lens precisely

Tripod

Optic sights

Lasers: future work

Blooming the camera with the 200mW laser has caused some damages to the camera (some pixels are now off).

What if we use some more powerful lasers?

Is it possible to remotely destroy the camera?

Agenda

How-to: infrared technology

Goal

To mask someone's face by flashing it with infrared.
We do not care about being recorded by the CCTVs. We just make sure not to be identified.

How-to: infrared technology (2)

From a webcam to an infrared camera... for a few euros

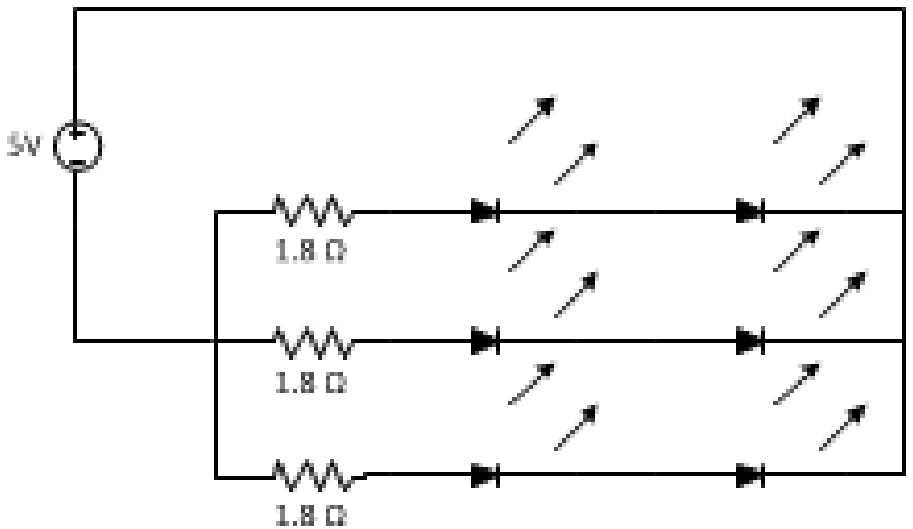
The webcam

Before ...

...and after modifications.

How-to: infrared technology (3)

CC vs. custom power supply



LEDs CC power supply

How-to: infrared technology (4)

CC vs. custom power supply

CC power supply: conclusion

- Not enough LEDs powered by a single 9V battery
- Not enough brightness
- Too much LEDs warming

$\Rightarrow$ CC power supply unsuitable for such a purpose

How-to: infrared technology (5)

CC vs. custom power supply

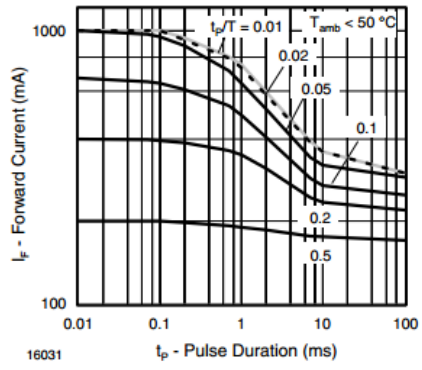


Fig. 3 - Pulse Forward Current vs. Pulse Duration

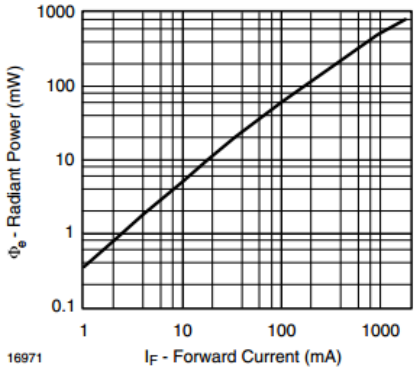


Fig. 6 - Radiant Power vs. Forward Current

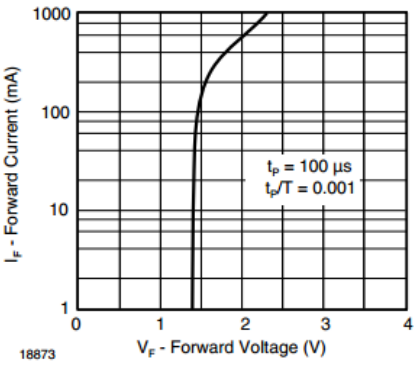


Fig. 4 - Forward Current vs. Forward Voltage

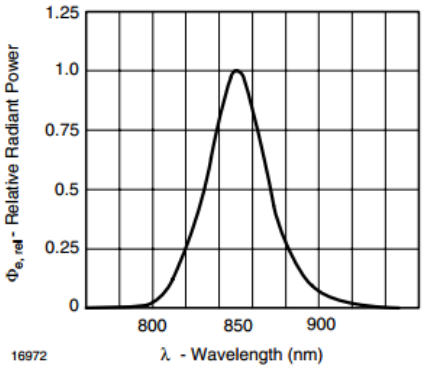
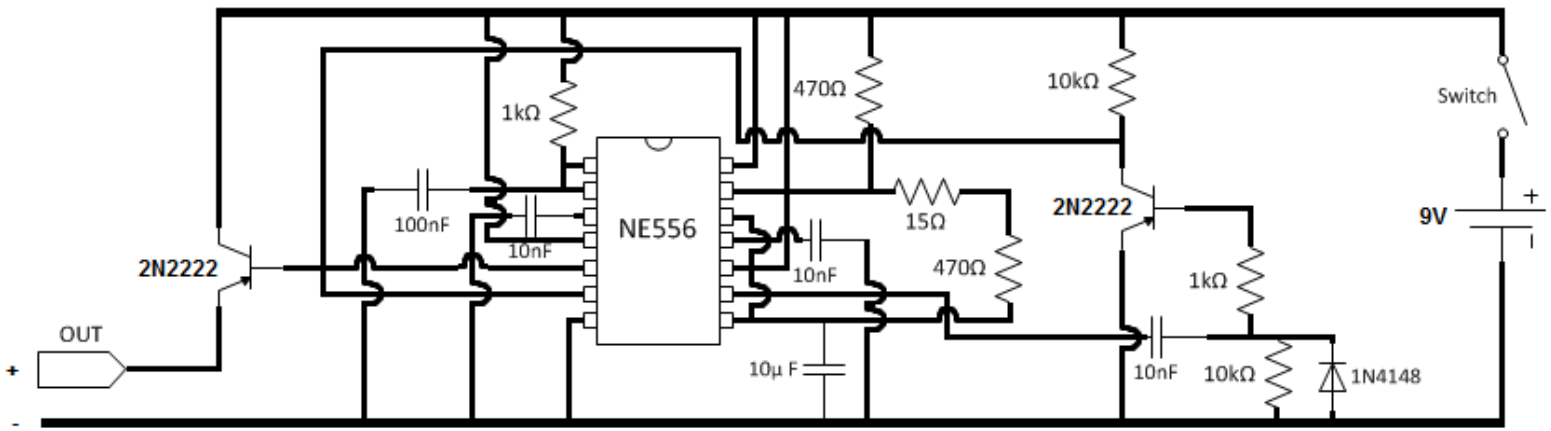


Fig. 7 - Relative Radiant Power vs. Wavelength

Extract from the LEDs datasheet

How-to: infrared technology (6)

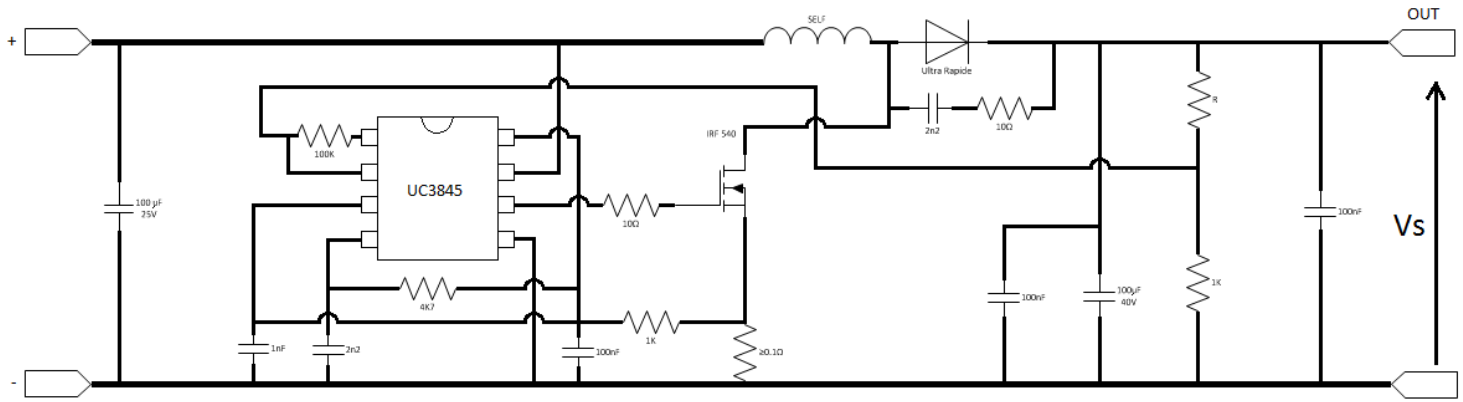
CC vs. custom power supply



A custom power supply based on NE556 chip

How-to: infrared technology (7)

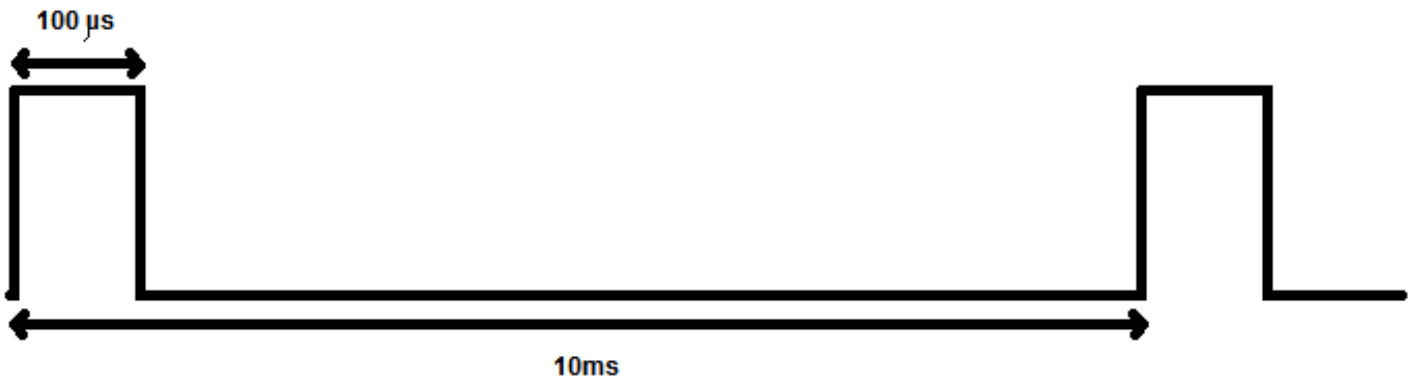
CC vs. custom power supply



A voltage booster, from 9 to 40V

How-to: infrared technology (8)

CC vs. custom power supply



The SMPS output

How-to: infrared technology (9)

CC vs. custom power supply

SMPS: conclusion

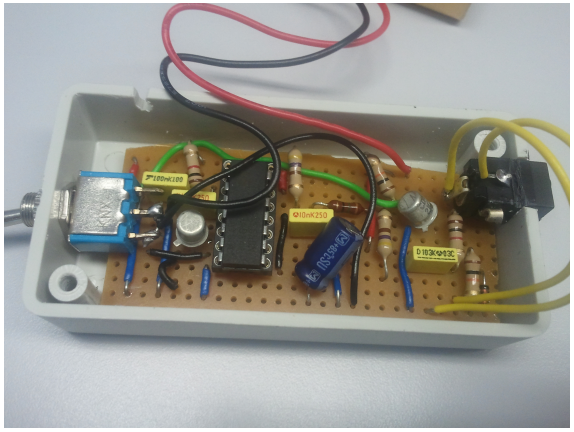
- More than 15 LEDs serially connected
- Maximum brightness
- No dangerous LEDs warming

$$\Rightarrow \text{LEDs optimal use}$$

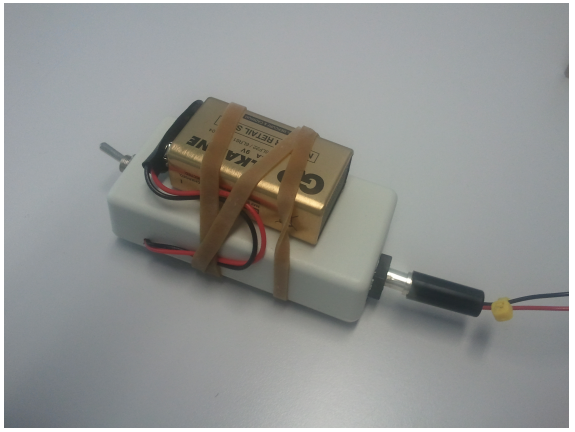
- Possible to hide all this in an innocent-looking item (e.g. necklace)

How-to: infrared technology (10)

Digital balaclava



The SMPS in ...



...and out.

How-to: infrared technology (11)

Digital balaclava

The result

Agenda

The tactical scheme

- A group of attackers want to operate in a given (urban) area, which is under CCTV surveillance.
- They want to evade the detection or identification during a limited period of time.
- The issue is how to combine previous single attacks into a combined one in order to make this area totally blind
  - for example a blind corridor to sneak from one point to another one, or to infiltrate an aera.
- How to do that with a limited number of ressources (human, money...)?
- Just use intelligence and graph theory.

Intelligence step: get the information

- Use our good friend *Google* and its minions (maps, streetview...)
- Many dedicated sites provide a huge amount of very detailed information for many areas/cities.
- Westminster city map of CCTVs.
- Let us show a few examples in Paris (`paris.sous-surveillance.net` and *streetview*).

Modelling the CCTV Network

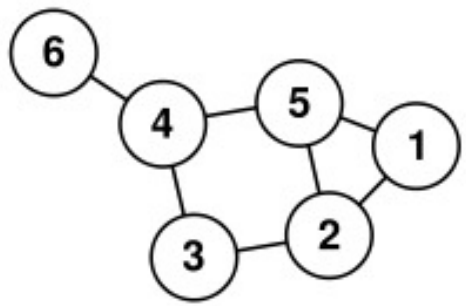
- The aim is to model and analyze the visibility connections between CCTVs.
- Use combinatorial optimization problems of the graph theory.
- CCTV networks can be modelled by graphs.
- Nodes of G, denoted $(n_i)_{1 \leq i \leq N}$ are representing CCTVs.
- Entries of the incidence matrix of G (its edges) are defined by:

$$a_{i,j} = \begin{cases} 1 & \text{CCTV } i \text{ is connected by a street to CCTV } j \\ 0 & \text{otherwise} \end{cases}$$

- You can use directed edges to describe the fact that CCTV i is monitoring CCTV j as well.

Modelling the CCTV Network (2)

- Normally, optimized implementation of CCTVs networks should be described by the *vertex cover* problem.

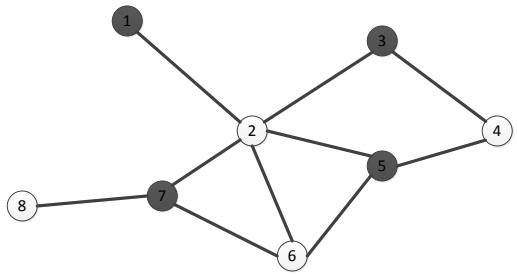


$\{2, 4\}$ is the maximal vertex cover (hemispheric CCTVs case)

- But security hysteria & commercial interests result in mass redundancy of CCTVs

CCTV subnetwork monitoring other CCTVs

- CCTVs monitoring other CCTVs are of critical interest (the first to manage).
- Search for the independent set within the graph or a subgraph (the area of operational interest).

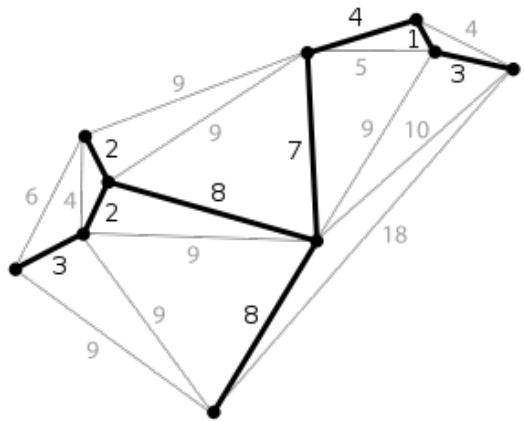


Subset of black vertices represents the independent set

- The general problem is NP-complete (untractable for large graphs; Robson's algorithm in $\mathcal{O}(2^{0.276.n})$).
- Can be solved in polynomial time (heuristics) for small subgraph or partial graphs (local area). Use routines *maximum_independent_set* and *maximum_independent_set* of *NetworkX*.

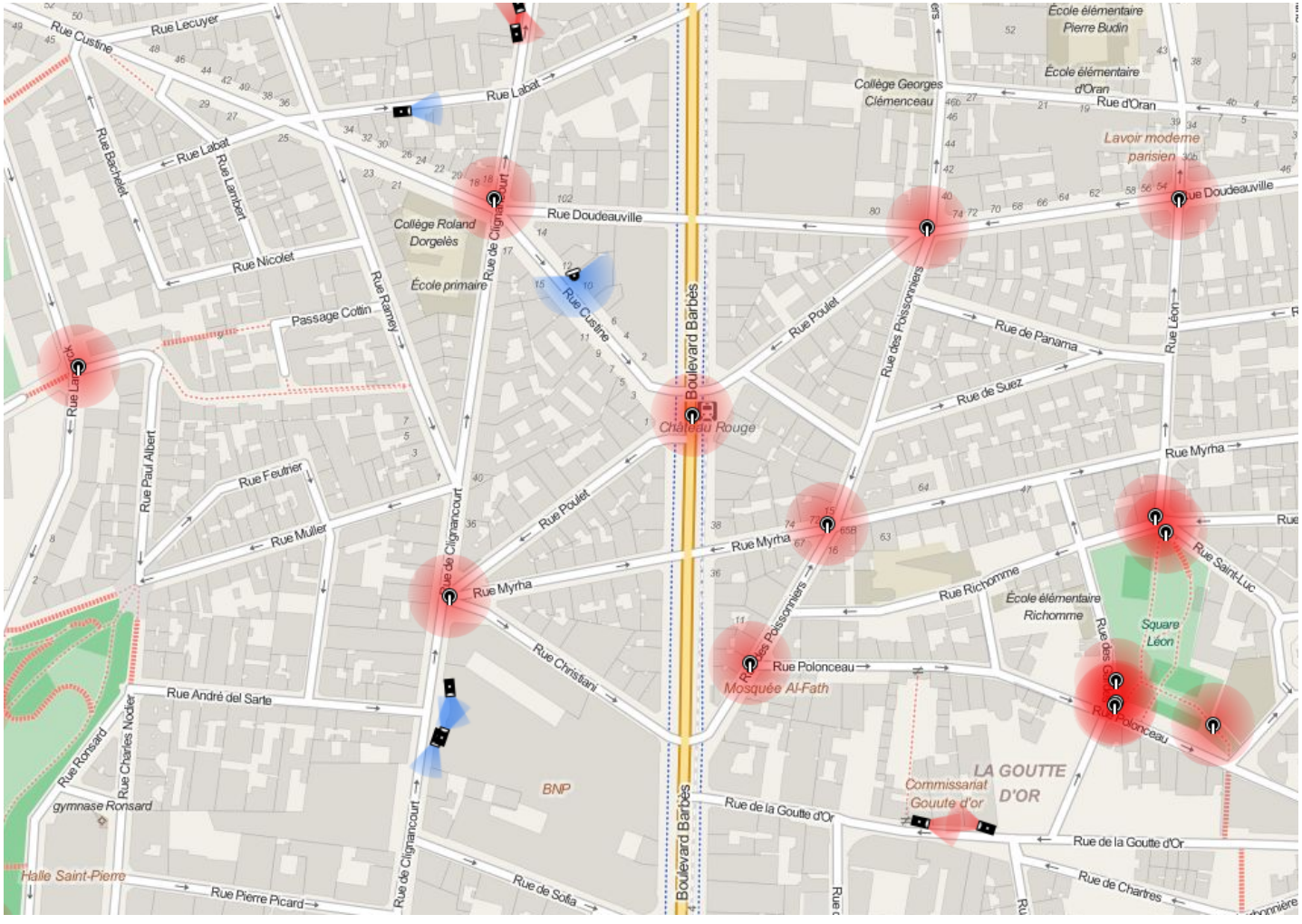
Creating blind corridors/areas

- The goal is to create a blind corridor or a blind (local) area.
- The solution is to consider the minimal Spanning tree problem for a partial graph or a subgraph corresponding to the area to manage.



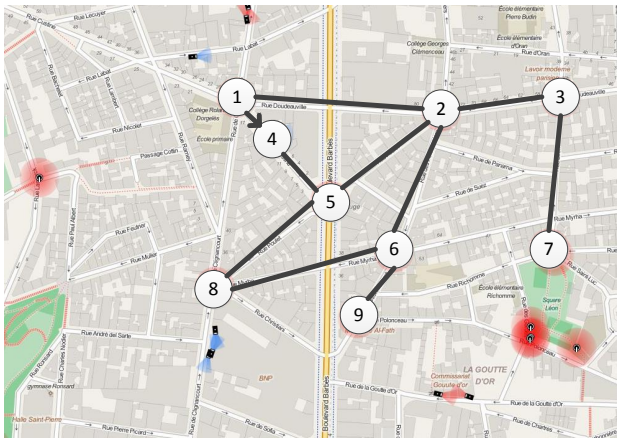
- The general problem has polynomial complexity (Kruskal algorithm in $\mathcal{O}(M.\log_2(N))$).
- Equivalently, we can consider the *graph matching* problem.
- Many other approaches and model at the attackers' disposal (*local clique problem, graph reduction techniques*...). Make just you operational thought precise and use graph theory.

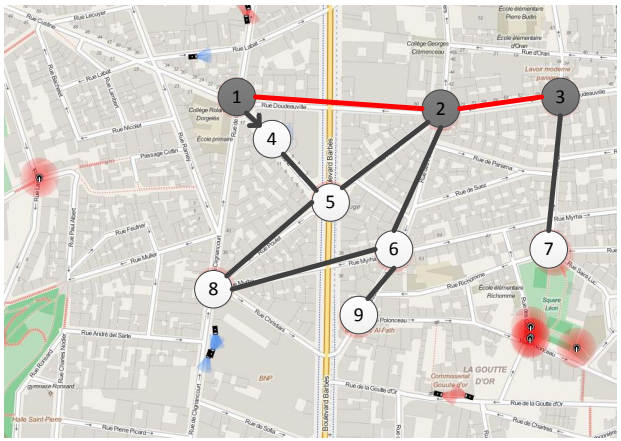
Illustration case in Paris

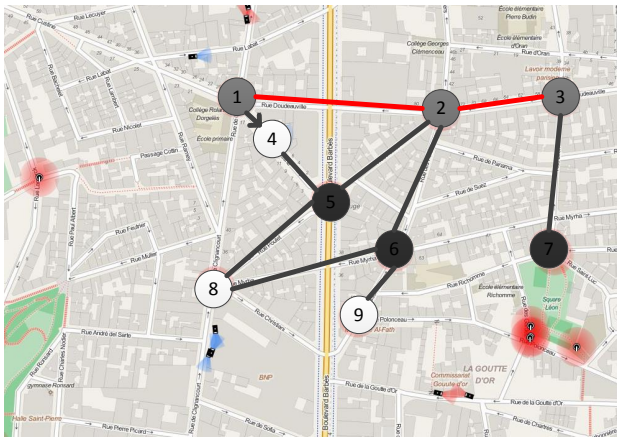


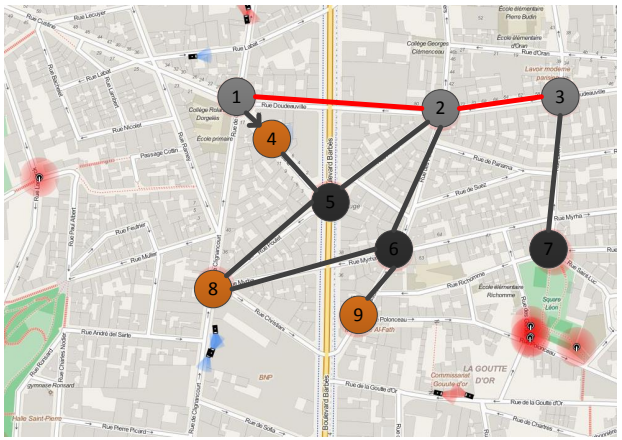
Somewhere in Paris

Illustration case in Paris









Agenda

Conclusion

- Most CCTVs are very weak regarding our attacks and many other techniques are possible (work under current development)
  - Not only CCTVs :-)
  - The realm of electronics and programming... but also algorithmic.
  - Do electronic and hardware hacking!
- CCTVs may be useful for mind peace but not for real security (at least for existing models).
- Vendors make easy profit by selling weak technology for a very high price.
- Decision-makers are already blind.

Thank you for your attention

{filiol,tscherrer}@esiea-ouest.fr

Questions?