META MERIANAE

Analyse Criminelle Informatique

Modélisation, automatisation et restitution

SSTIC 2004

02 Juin 2004

Thomas «DomTom» DUVAL thomas.duval@supelec.fr

Bernard JOUGA bernard.jouga@supelec.fr

Laurent ROGER roger@celar.fr

Introduction

« Tout individu à l'occasion de ses actions criminelles en un lieu donné, dépose et emporte à son insu des traces et des indices. »

Edmond LOCARD

(père fondateur de la police scientifique)

1910

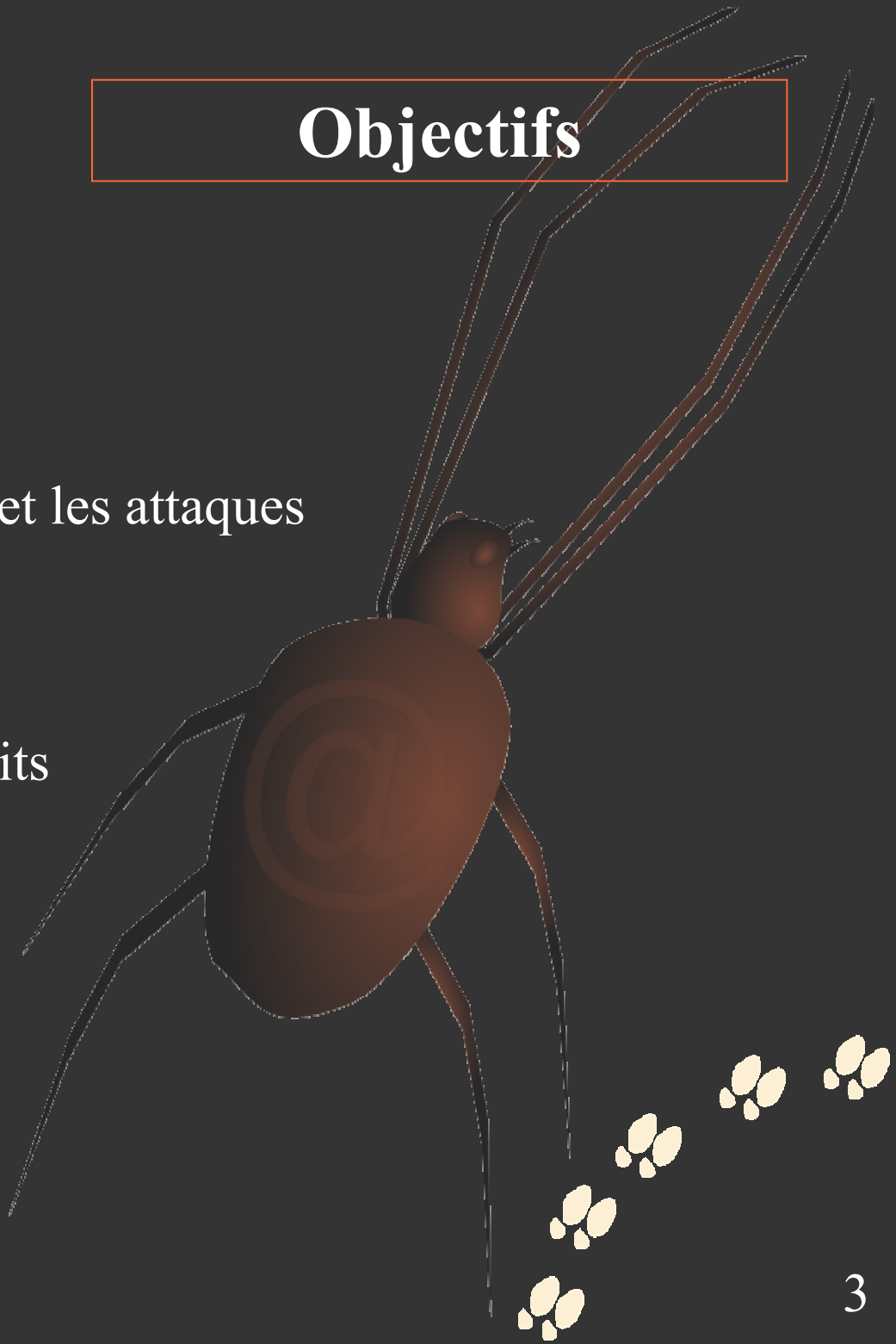
Forensics

Objectifs

Déterminer les dégats et les attaques

Réparer les dégats

Trouver l'auteur des faits



Forensics

Méthodes

Analyse des variables éphémères

Analyse de la topologie réseau

Analyse des fichiers d'audit

Analyse du système (fichiers cachés / supprimés)

Analyse de la composante humaine

Forensics

Remarques

Sonner l'alarme

MINISTÈRE DE LA DÉFENSE

« **Pull the plug !** »

- pour arrêter l'attaquant
- pour garder les preuves intacts

Méthodologie

Objectifs :

- Aider les enquêteurs dans leurs investigations
  - sur les attaques
  - sur les attaquants (profils)

Méthodes :

- Sous la forme d'un système expert
- Utilisant les Réseaux Bayésiens pour l'inférence

Méthodologie

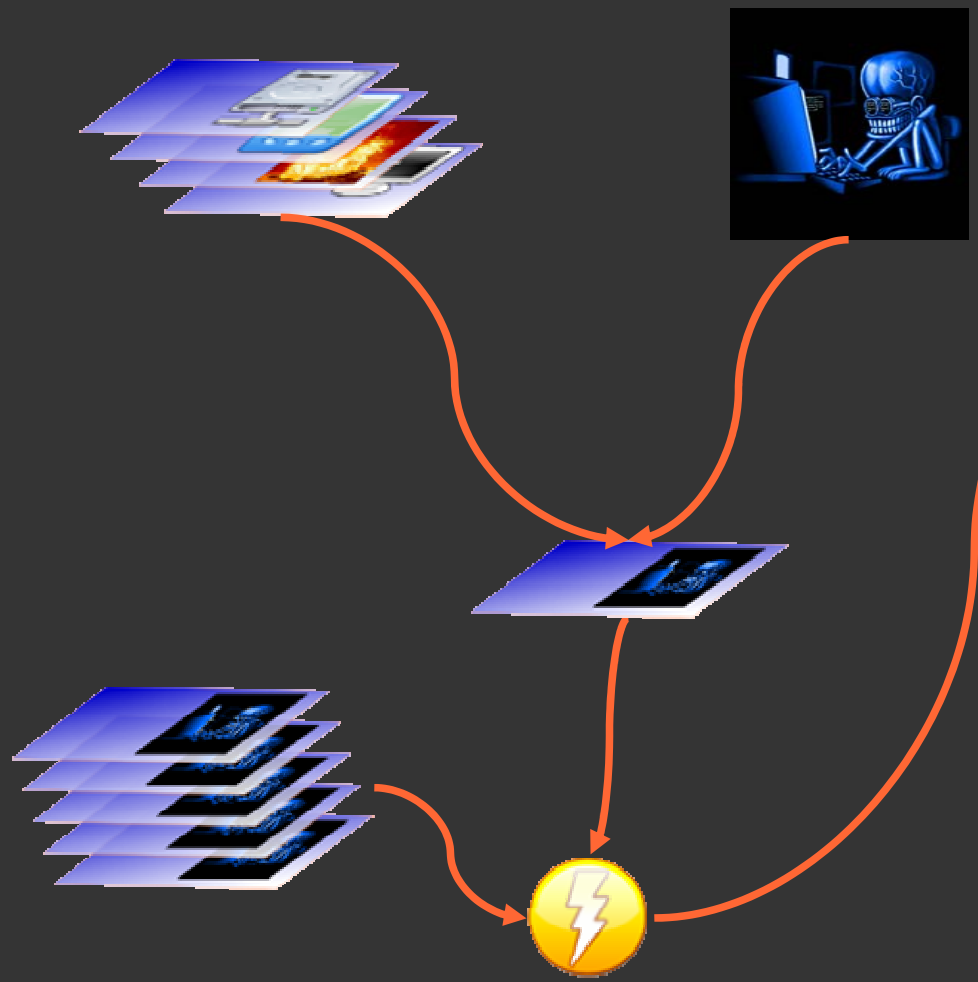
Attaques

1 plan =

1 attaque
1 composant

Méthodologie

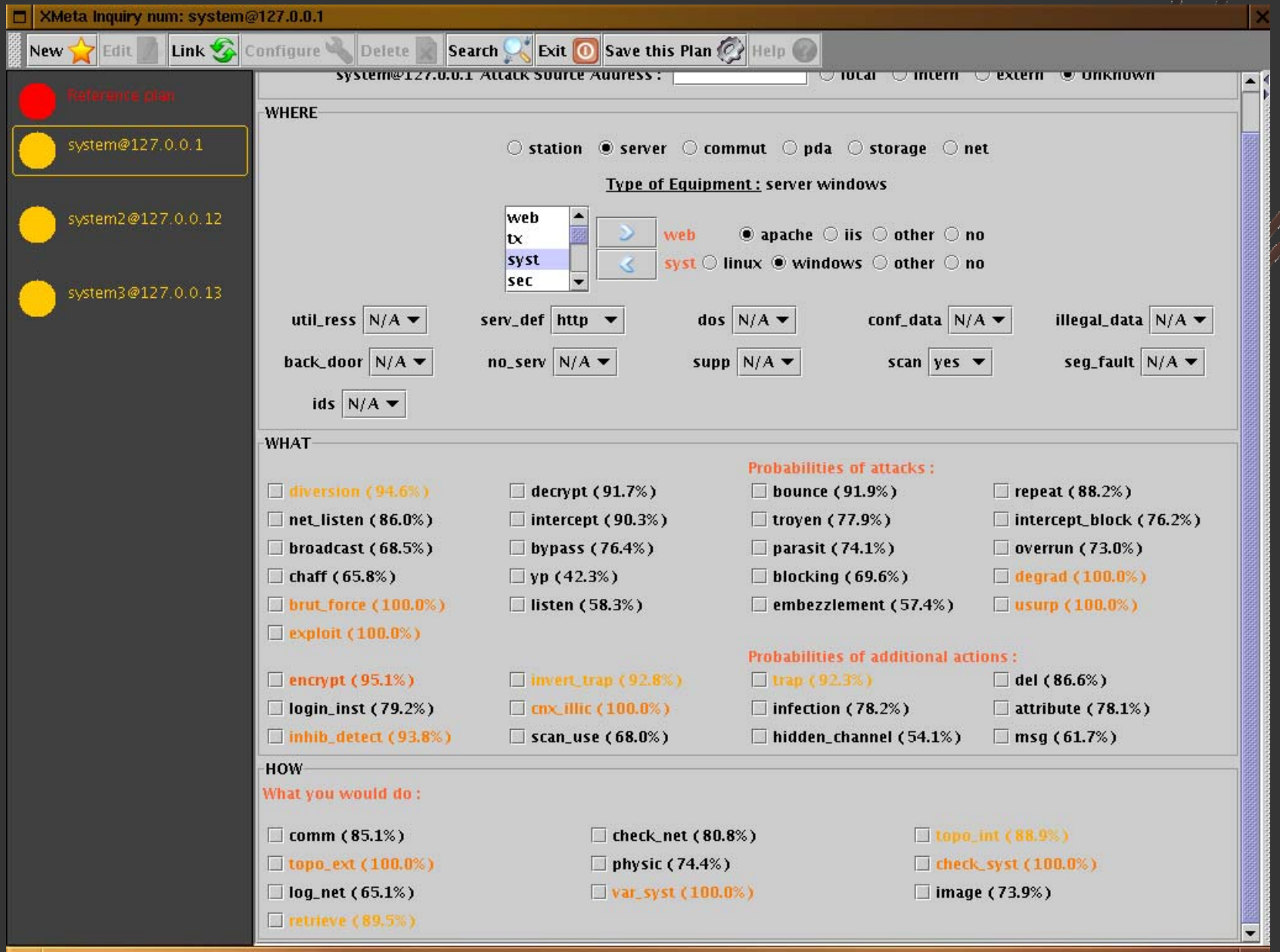
Attaquants



- **Découvrir l'auteur**
- **Découvrir ses actions possibles**
- A la manière des *profilers* américains

Méthodologie

Travaux en cours



JAVA

API BNJ

BIF

CFXR

Travaux futurs

- Gestion des profils
- Etude des techniques de comparaison de RB
- Exploitation des bases de vulnérabilités

- Travail sur des données réelles (avec la DGA)

SSTIC 2004

02 Juin 2004

QUESTIONS ?

http://www.rennes.supelec.fr/ren/perso/tduval/

Thomas «DomTom» DUVAL thomas.duval@supelec.fr

Bernard JOUGA bernard.jouga@supelec.fr

Laurent ROGER roger@celar.fr