The EU Research Efforts on Detecting and Analyzing Emerging Threats: The WOMBAT and FORWARD Projects

Engin Kirda
Associate Professor, Institute Eurecom

An event organised by the European Commission (DG INFSO)
& the South Korean Ministry of Knowledge Economy (MKE)

December 1-2, 2008
Radisson SAS Royal Hotel
Brussels, Belgium

MKE 지식경제부
Ministry of Knowledge Economy

European Commission
Information Society and Media

Detecting and Analyzing Emerging Threats

- Internet security has become part of everyday life where security problems impact practical aspects of our lives
- Understanding the details of Internet-based attacks is a prerequisite for the design and implementation of secure systems and services
- Cybercrime has become a business!

Online Crime is a Business Now

- Klikparty, 2007

Online Crime is a Business Now

- Klikparty, 2007

WOMBAT and FORWARD

- WOMBAT (Worldwide Observatory of Malicious Behaviors and Attack Threats)
  - Budget ~4.4 m€, for 3 years
  - **Aims to build an automatic, global network which can perform early warning, automatic classification and analysis of malware and exploits as they propagate, or are used, worldwide**
  - **http://www.wombat-project.eu/**
- FORWARD (Coordination Support Action)
  - Budget: ~900 k€, for 2 years
  - **EU-wide initiative to promote the collaboration and partnership between Academia and Industry in their common goal of protecting ICT infrastructures**
  - **http://www.ict-forward.eu/**
- Both started in January 2008

WOMBAT Motivation

- Cyber-crime becomes harder to battle
  - Malware specifically designed to defeat today's best practices
  - Organization is consolidating malicious activity into a profitable professional endeavour
- Data collection and sharing is limited
  - Collection initiatives are heterogeneous
  - Privacy or confidentiality limits sharing
  - Data structure and analysis remains private
- No investigation framework exists for consistent and systematic malware analysis

The WOMBAT Consortium

EURECOM
Sophia Antipolis

orange™

TECHNISCHE UNIVERSITÄT WIEN
VIENNA UNIVERSITY OF TECHNOLOGY

TU WIEN

WOMBAT

NASK

POLITECNICO DI MILANO

symantec.

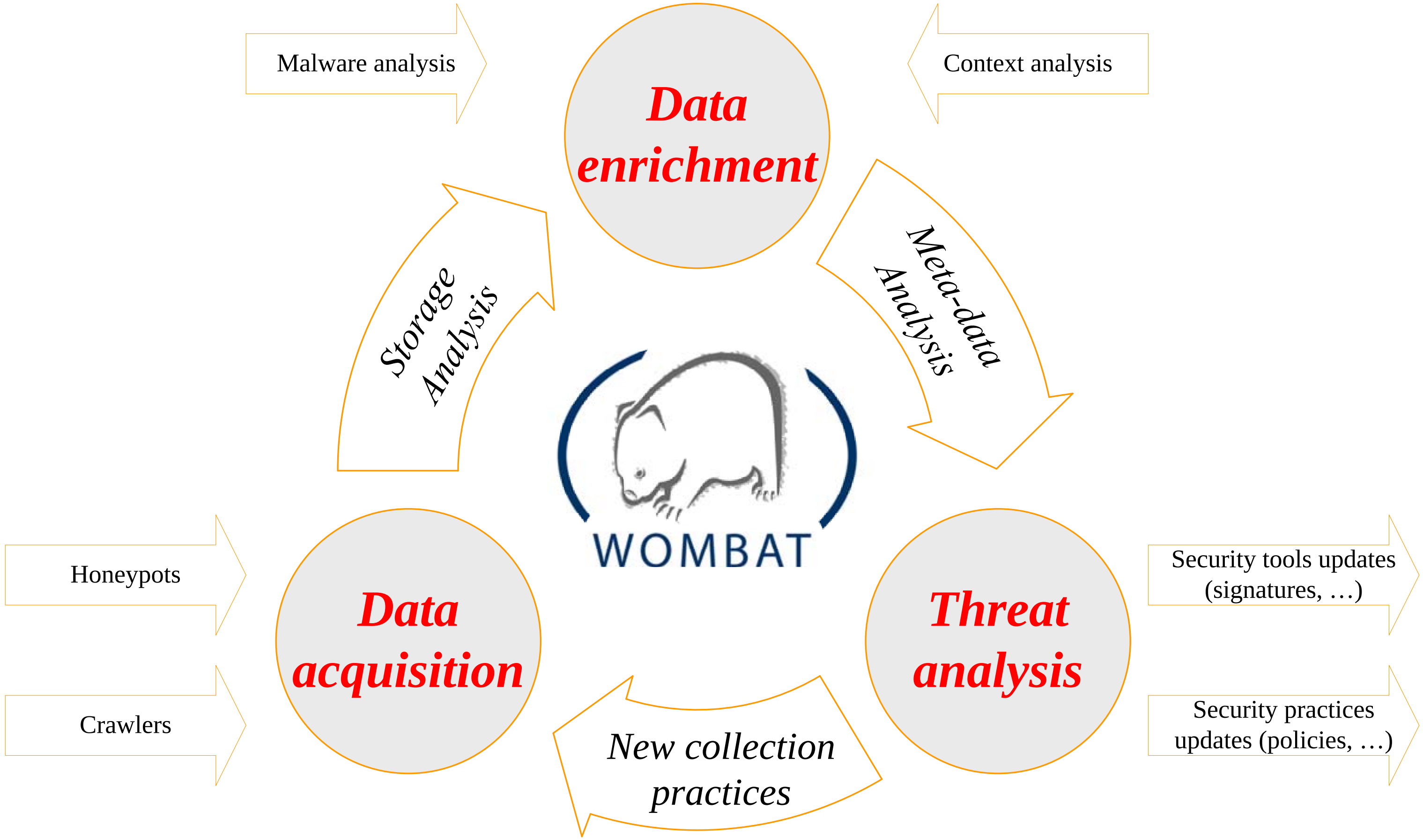
vrije Universiteit

FORTH

A*STAR
Institute for Infocomm Research

HISPASEC SISTEMAS

WOMBAT Main objectives and principles



Malware analysis

Context analysis

Data enrichment

Storage Analysis

Meta-data Analysis

WOMBAT

Honeypots

Crawlers

Data acquisition

Threat analysis

Security tools updates (signatures, …)

Security practices updates (policies, …)

New collection practices

WOMBAT Project results and innovation

- New data gathering tools
  - Advanced features (high interaction, real-time analysis)
  - New targets (wireless, bluetooth, RFID, …)
- Tools and techniques for characterization of malware
  - Malware-based analysis
  - Contextual analysis
- Framework and tools for qualitative threat analysis
  - Early warning systems

The FORWARD Project

- FORWARD aims to:

  - Promote partnership and collaboration between researchers from academia and industry in ICT protection

  - We deal with cyber-threats such as malicious code (worms, botnets, spyware, etc.)

  - Our main goal is to identify, network and coordinate the ongoing multiple research efforts

The FORWARD Consortium

EURECOM
Sophia Antipolis

AVANCEZ
1829

TU
WIEN

Technische Universität Wien

Vienna University of Technology

forward

IPP
BAS

vrije Universiteit

FORTH

FORWARD Working Groups

- Smart Environments
  - Identifying and analyzing emerging and future threats in areas such as: wireless and wired networks, ambient intelligence environments, cellular telephony networks, vehicular networks, RFID, network monitoring, the Internet of things
- Malware and Fraud
  - Identify all aspects of malicious code and fraudulent activities in ICT networks. This includes the complete life cycle of online fraud and malware
- Critical Systems
  - Identify emerging threats in critical systems (e.g., health systems, power control systems, etc.)
- Anyone can participate!

Possibilities for International Collaboration

- International Collaboration is welcome in WOMBAT and FORWARD
- Data Collection and sharing
  - We are encouraging everyone participating in FORWARD and WOMBAT workshops to share their security data for research
  - e.g., IDS logs, phishing data, fraud information, malware samples
- Participation of academic researchers and industrial stakeholders in the FORWARD working groups
  - Meet and talk to international experts [from the EU and the US]
  - We would welcome participation from South Korea!
  - Next large workshop to be organized in France in September 2009

Conclusion

With WOMBAT and FORWARD, the EU is funding research in detecting, analyzing and mitigating current threats such as botnets, worms, viruses and Trojan horses

  - Our research and collaboration aims at combating cyber-crime

- WOMBAT and FORWARD are open to international participation
  - Data sharing, participation in working groups, workshops