Upcoming Threats in Cyber-crime
The research issues

Neil Mitchison, Marc Wilikens,
Neil.Mitchison@jrc.it ; Marc.Wilikens@jrc.it
Tel: +39 0332 785325

eAWARE, Rome November 2003

http://www.jrc.cec.eu.int

Cyber-crime: risk analysis

- Opportunist crime and organised crime
  - Vulnerability analysis
    Where are the weak points?
    Where are the lures?
    How do the defences work? (New vulnerabilities?)
- Old crimes made easier; new crimes; new ways to commit familiar crimes
  e.g. “Nothing succeeds like success” – identity theft
- Information as object and also as means of crime
  e.g. Cryptographic protection
- Cyber-security as part of overall security
  - Insider/outsider alliances

Systemic solutions, e.g. biometrics

- Systemic vulnerability analysis needed
  but also testing!
- Security vs. Useability
  - Users' objective is to use the system; if that means bypassing the security protection, they'll do so
  - How does the system get used in practice?
    - False positives from security protection
    - Single barrier or defense in depth (false negatives?)
    - The routine fixes: "I've forgotten my password"
    - The necessary (and unnecessary) back doors
    - Social engineering among the administrative community

Cyber-crime and cyber-security: the JRC

Technical advice for policy support

- International initiatives in combating cybercrime (with Europol, Interpol):
  - Characterisation of high-tech crime (e.g. identity theft)
  - Methodology for gathering verifiable electronic evidence of illicit activities (CTOSE project)
  - Training course with accession countries on computer forensics
- Technology Roadmaps:
  - computer attacks early warning needs, critical information infrastructure protection, ambient intelligence security and privacy
- Test bed to evaluate privacy risks in support of EU data protection regulation
- Pilot development of EEJ-Net: European Extra-Judicial Network for consumer protection, cross-border complaints and disputes
- Complementary application projects on secure ICT
  - E-Health: DRIVE (IST)
  - E-Voting: vulnerability of Internet voting to severe attacks

CTOSE:
Electronic evidence for cyber-crime investigations

Objective: a methodology: how to identify and handle electronic evidence

Timescale: December 2001 – September 2003

Team: JRC *(project leader)*

Alcatel (CERT-IST) (*experience of current practices)*

QinetiQ (formerly DERA), UK (*computer forensics)*

3 Universities: Namur (CRID) *(legal aspects);* St. Andrews (*e-management);*

Stuttgart (Fraunhofer) *(IT system building)*

Special Interest Group including industry and law enforcement bodies

Deliverables: User requirements analysis; legal advisor; process model; cyber-crime advisory tool (C*CAT); XML evidence specification; pilot demonstrator of attacks and responses

Follow-up: Research network; roll-out and market testing project; proposal for an Electronic Evidence Foundation