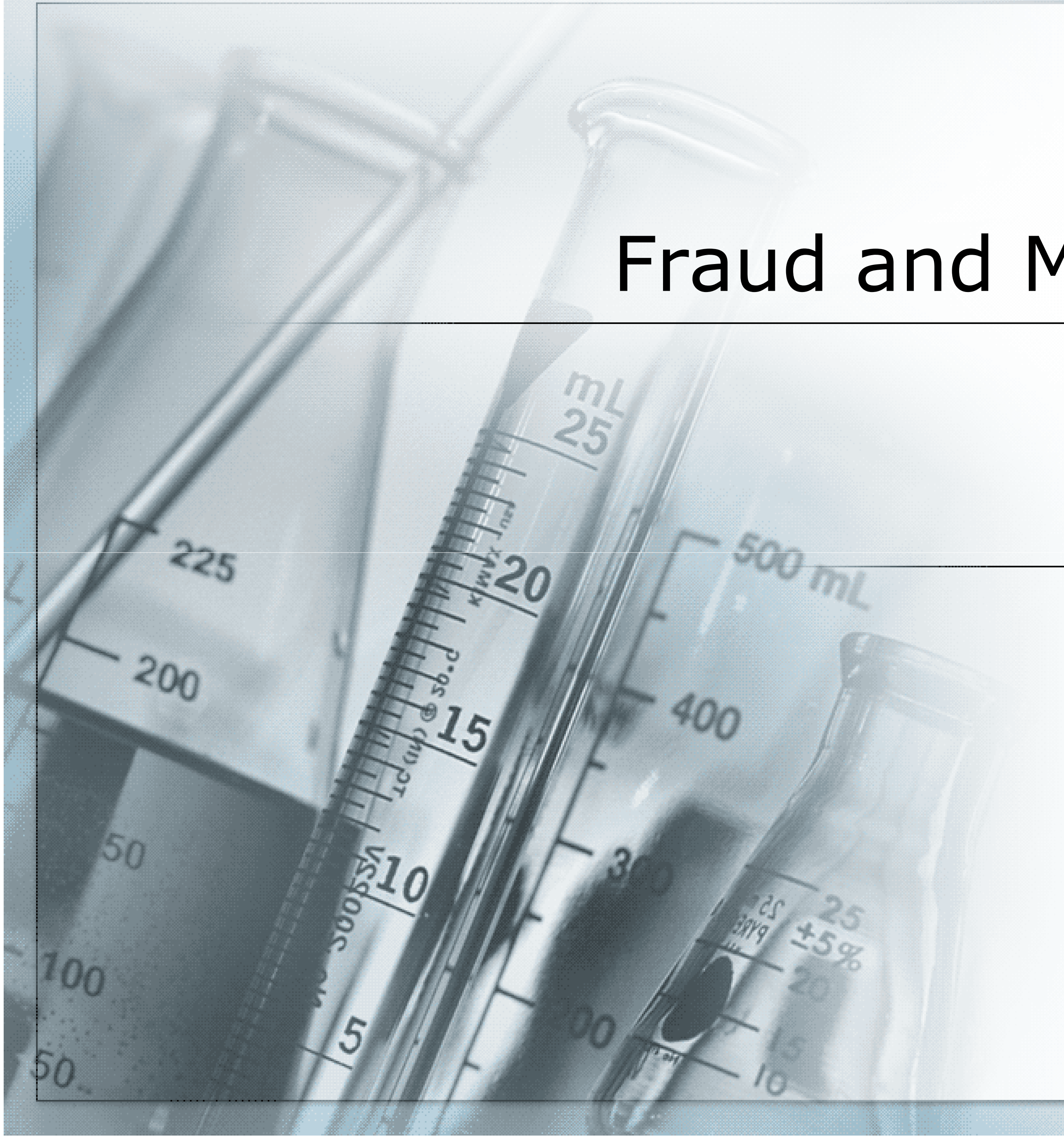

Fraud and Malware

EC2ND 2008

Forward Project

The business of cybercrime

- Moving from “Hack for Fun” to “Hack for Profit”
- Malware developers/users are supported by traditional crime organizations
- Traditional fraud mechanisms combined with technological knowledge led to a well-established underground economy.

Online Crime is a Business Now

Klikparty, 2007

Online Crime is a Business Now

Klikparty, 2007

Solution Approaches

- Surveillance of underground Channels
  - IRC, Web Pages, etc..
- Understanding the internal structure
  - Who buys what?
  - Payment?
- Disrupting possible weak links
  - From a Web Page to the advertising Spam Mail

Trends in Malware

- New propagation vectors
  - From mail to social networks
- New stealth mechanisms
  - Malicious hardware components
  - CPU microcode
- Advanced Bot nets
  - Strong cryptography
  - Hidden channel communication

Impact of new technologies

- IPv6
  - Scanning
  - NAT
- Mobile devices (GPS, etc…)
  - Privacy issues
  - Payment
- Virtualization
  - Jail breaking
- Social networks and online communities
  - Identity theft