Introduction: Grid & Security

Remi Mollon, CERN

CERN ROC Security Contact

Operational Security Coordination Team

EGEE'07, Budapest

1st October 2007

www.eu-egee.org

The risks

- **Impact on the reputation of the project and of the partners**
- **Launch attacks on other sites (DDoS, Spam, ...)**
  - Large distributed farms of machines
- **Damage caused by viruses, worms, etc.**
  - Highly interconnected and novel infrastructure
- **Service disruption by exploitation of security holes**
  - Complex, heterogeneous and dynamic environment
- **Illegal or inappropriate distribution or sharing of data**
  - Massive distributed storage capacity

The dark side of the force

- **Cyber attacks were led by individuals for a long time**
  - motivated by fame and self-satisfaction
  - small-scale attacks
- **Organised crime syndicates are now in the arena**
  - motivated by money
  - large-scale attacks
  - professional attackers
  - better-designed and smarter malicious code
- **Spams, phishing, illegal materials, extortion, ...**

Malware kits

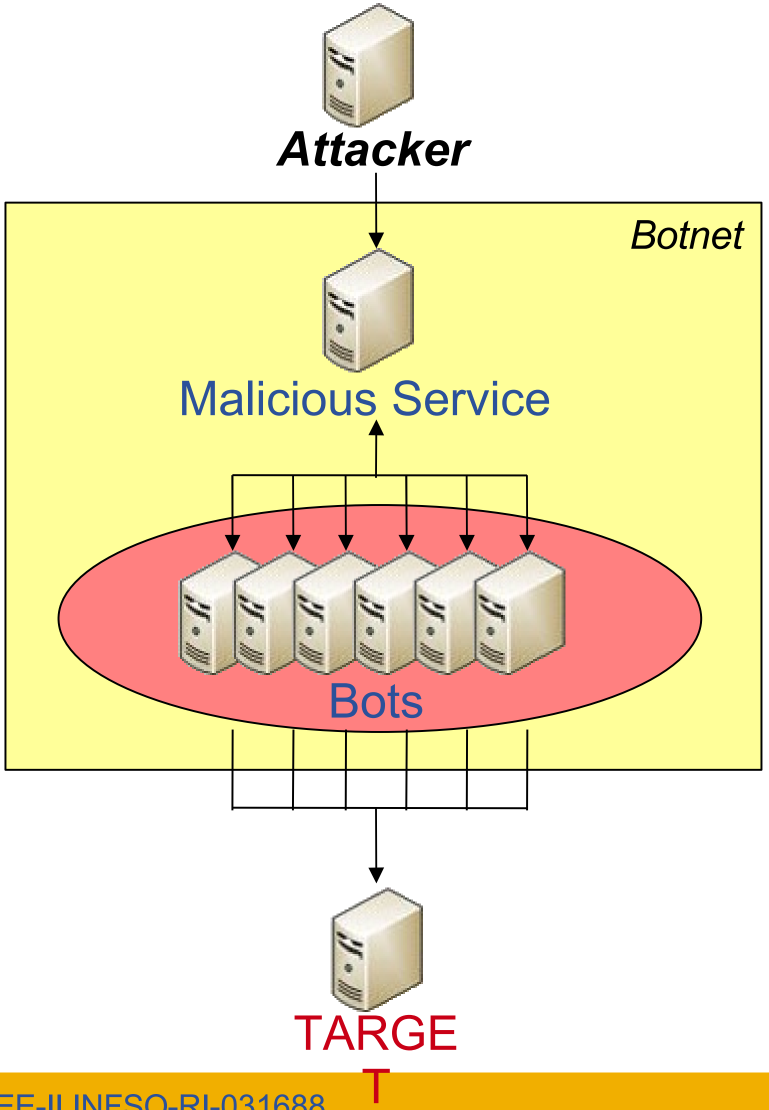
- **No need to be a security expert**
  - Graphical interface
  - Highly customisable
  - BUT sophisticated
- **MPack**
  - Professional PHP-based malware kit
  - Commercial software
    - sold from $500 to $1,000
    - provided with 1-year technical support
    - regular updates of the software and exploited vulnerabilities (from $50 to $150)
    - can be enhanced by extensions

Storm botnet

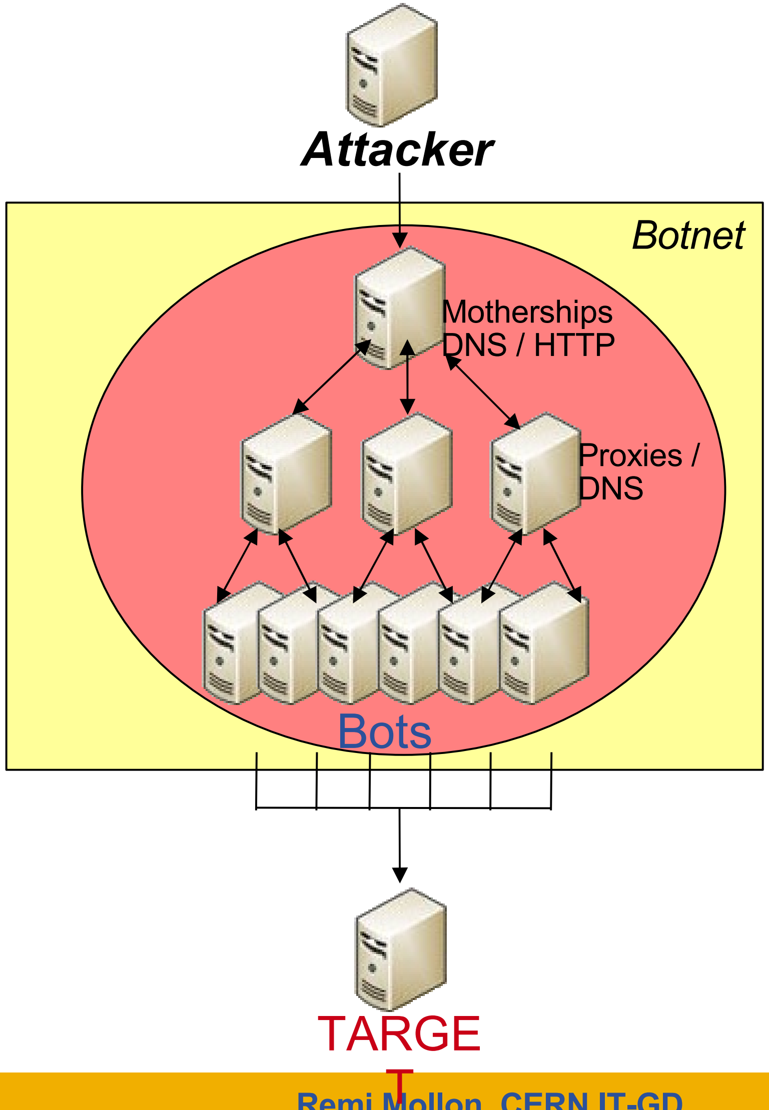
- **Massive network of computers linked by Storm worm**
- **Estimated to be composed of as many as 1,000,000 to 10,000,000 “bots”**
  - Powerful enough to force entire countries off the Internet
  - Do you still consider EGEE as a big Grid ?
- **Uses the “Fast-Flux” technology to be more difficult to locate and take down**
  - Large number of servers (bots can also be servers)
  - Fast changing, proxied malware source and DNS records
    - Load balancing based on availability, bandwidth, etc.
    - Round robin
    - Short time to live
  - Authoritative DNS server can change as well

Storm botnet (2)

Classic Botnet



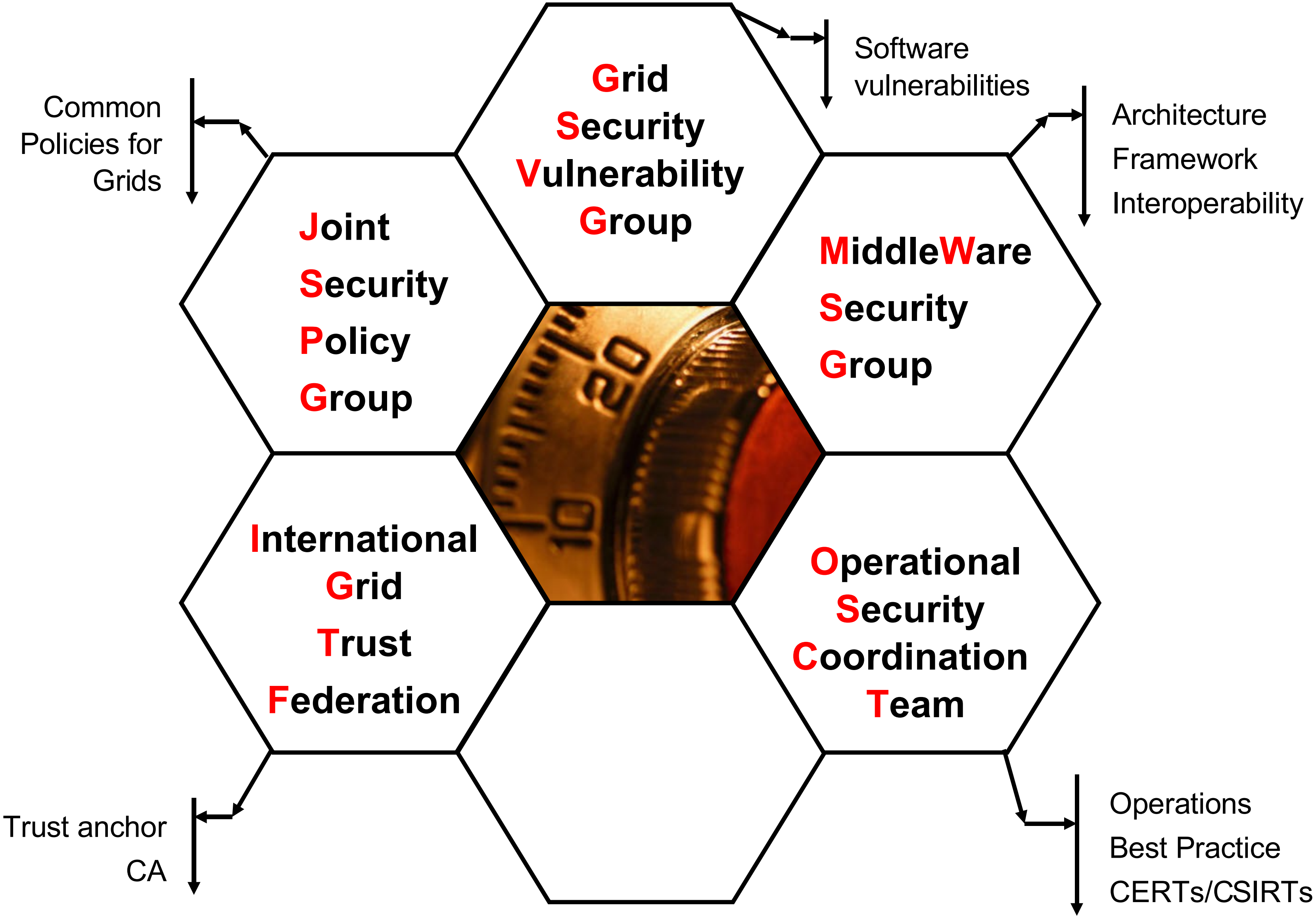
Fast-Flux Botnet



Impacts on Grid

- **Grid middleware services aren't as mature as other traditional network services**
- **Grid is a valuable target for attackers**
  - Plenty of powerful distributed hosts
  - High bandwidth connection
- **Grid is also particularly exposed**
  - Transparent access/attack propagation between sites
  - Large number of identical hosts (at least for OS)
- **Attackers choose the easiest way**
  - Heterogeneous skills, staffing and security standards
- **So far no "grid incident" (= where the grid is the attack vector)**
  - ... but ***WILL*** happen!

Security groups



Grid Security Vulnerability Group

Software vulnerabilities

Joint Security Policy Group

Common Policies for Grids

MiddleWare Security Group

Architecture
Framework
Interoperability

International Grid Trust Federation

Trust anchor
CA

Operational Security Coordination Team

Operations
Best Practice
CERTs/CSIRTs

(Image from Ake Edlund)

OSCT

- **Operational Security Coordination Team**
- **Three main activities**
  - Incident Coordination
  - Incident Response improvement
    - Incident Response Scenarii
    - Security Service Challenges
    - ...
  - Security monitoring
  - Best practice and dissemination
    - Trainings
    - Security RSS feed
      - *http://rss-grid-security.cern.ch/rss.php*

Security RSS feed

- **Organised in several subgroups**
  - Grid Security
  - System Housekeeping
  - System Monitoring
  - System Testing
  - Policies and Documentations
  - Intrusion Detection Systems
- **Top 5**
  1. System Housekeeping – Applying security patches
  2. System Housekeeping – Disabling root login with password
  3. System Housekeeping – Disabling and uninstalling unneeded services
  4. System Monitoring – Central syslog server
  5. System Housekeeping – Configuring a system-level firewall

Conclusion

- **Cybercrime is now professionally organised**
- **Attackers need CPUs, bandwidth and high availability**
- **...hence grids are becoming a valuable target for attackers**
  - Each site has to take care of its host security
  - There is no secure Grid without secure sites
- **Some groups exist to help users and sites to make the Grid as secure as possible**
  - Don't hesitate to contact the corresponding group if you need help!

Support contacts

- **Vulnerability reporting**
  - grid-vulnerability-report@cern.ch
- **Incident reporting**
  - your **local** security contact
  - project-egee-security-support@cern.ch
    - if your local security contact isn't available
  - Incident response procedure
    - https://edms.cern.ch/document/867454/
- **Operational security issues**
  - project-egee-security-support@cern.ch