La Sicurezza e la qualità dei dati nella Gestione dell'impresa

DIPARTIMENTO
DI INFORMATICA

SAPIENZA
UNIVERSITÀ DI ROMA

Luigi V. Mancini
mancini@di.uniroma1.it
Tel 06-4991-8421 or 8537

Information security

Protecting **information** and **information systems** from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction in order to provide:

- Integrity
- Confidentiality
- Availability

Information Security (2)

- Public and private businesses manage a great amount of confidential information about their employees, customers, products, research, and financial status.
- Protecting confidential information is a **business**, **ethical** and **legal** requirement.
- For the *individual*, information security has a significant effect on **privacy**.

Master


master universitario di primo livello
Master in Sicurezza dei Sistemi e delle Reti
Informatiche per l'Impresa e la Pubblica Amministrazione
master universitario di secondo livello
Master in Governance e Audit
dei Sistemi Informativi
master universitario di secondo livello
Master in Gestione della Sicurezza
Informatica per l'Impresa e la Pubblica Amministrazione

ISO 27001

- It formally specifies a management system that is intended to bring information security under explicit management control
- Benefits of compliance:
  - Improved effectiveness of Information Security
  - Senior Management takes ownership of Information Security
  - Focused staff responsibilities
  - Better awareness of security
  - Combined resources with other Management Systems (es QMS)
  - Mechanism for measuring the success of the security controls

Critical infrastructures and citizens services

Cyber Security

- USA “Cybersecurity Act of 2010 - S. 773”
- “Cyberspace is a vital asset to the nation and the United States should protect it.”
- More than 85% of the digital infrastructure is owned and operated by the private sector in US.
- The main objective of the bill is to increase collaboration between the public and the private sector on the issue of cyber security.

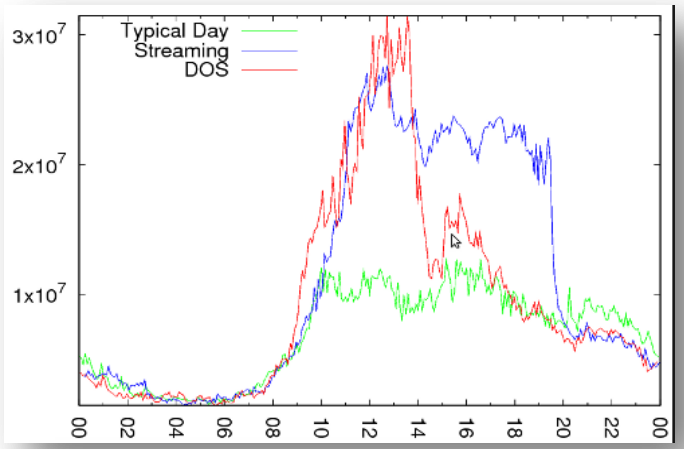
The ExTrABIRE project, Final Conf. June 18, 2012

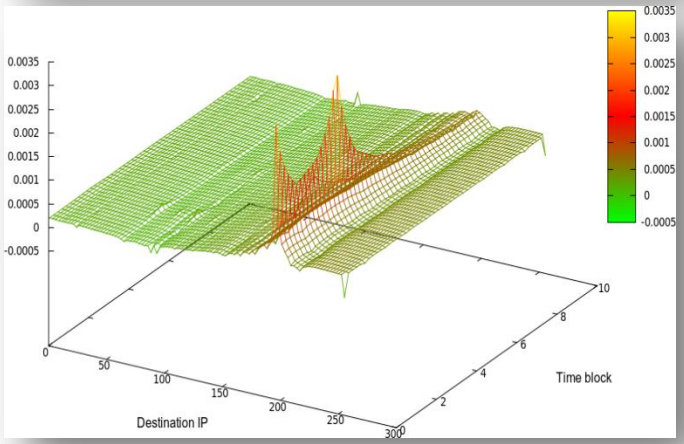
➢ **Exchanged Traffic Analysis for a Better Internet Resiliency in Europe – ExTrABIRE CIPS 2009 II Action Grants**

➢Evaluate the overall ***resiliency*** of internet infrastructure of a Member State

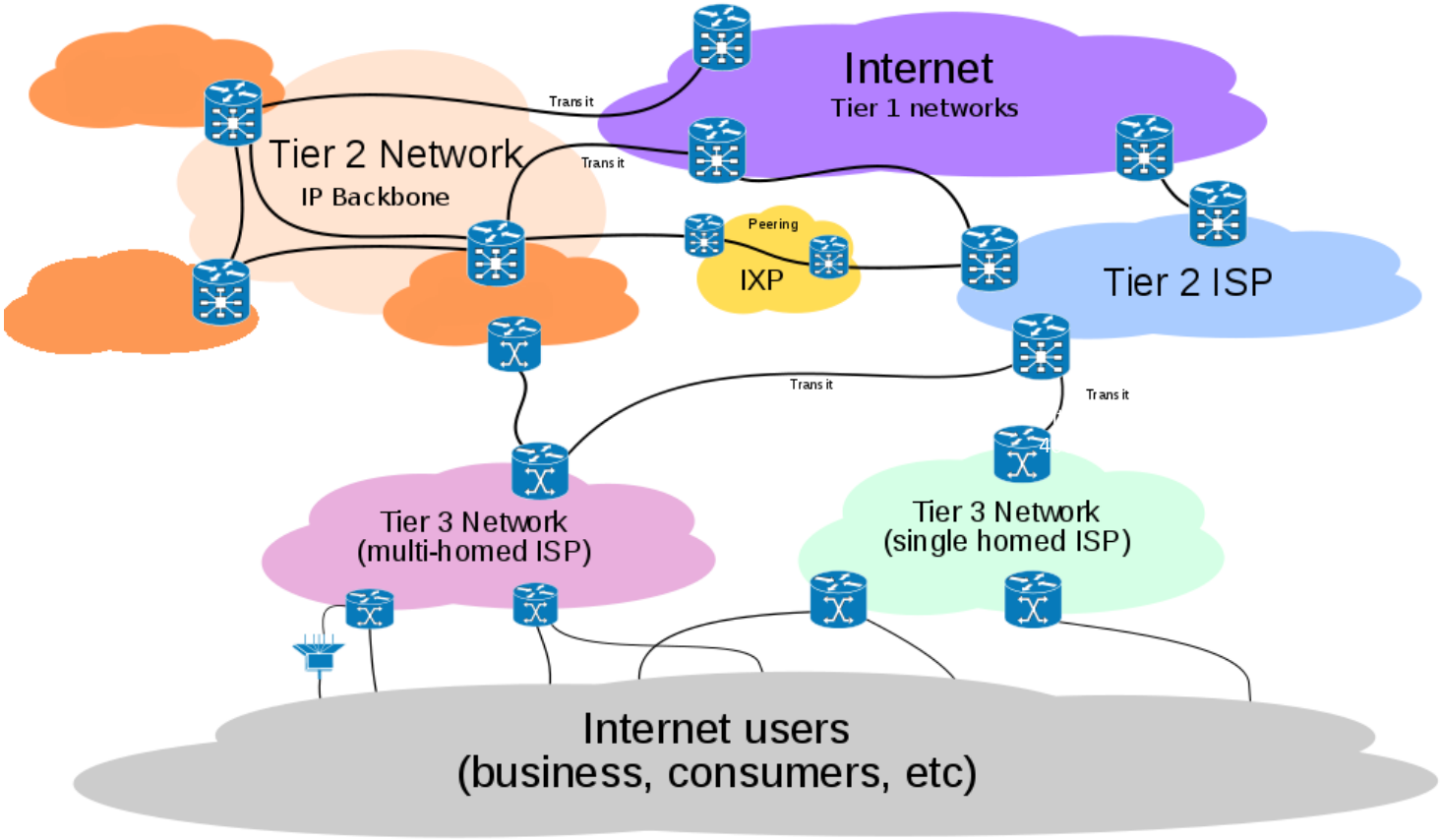
➢ Assess the impacts of a coordinated ***cyber-attacks***

➢ Develop a national internet ***contingency plan***:
- ➢ identification of processes and procedures;
- ➢ organizational issues;
- ➢ technical countermeasures.



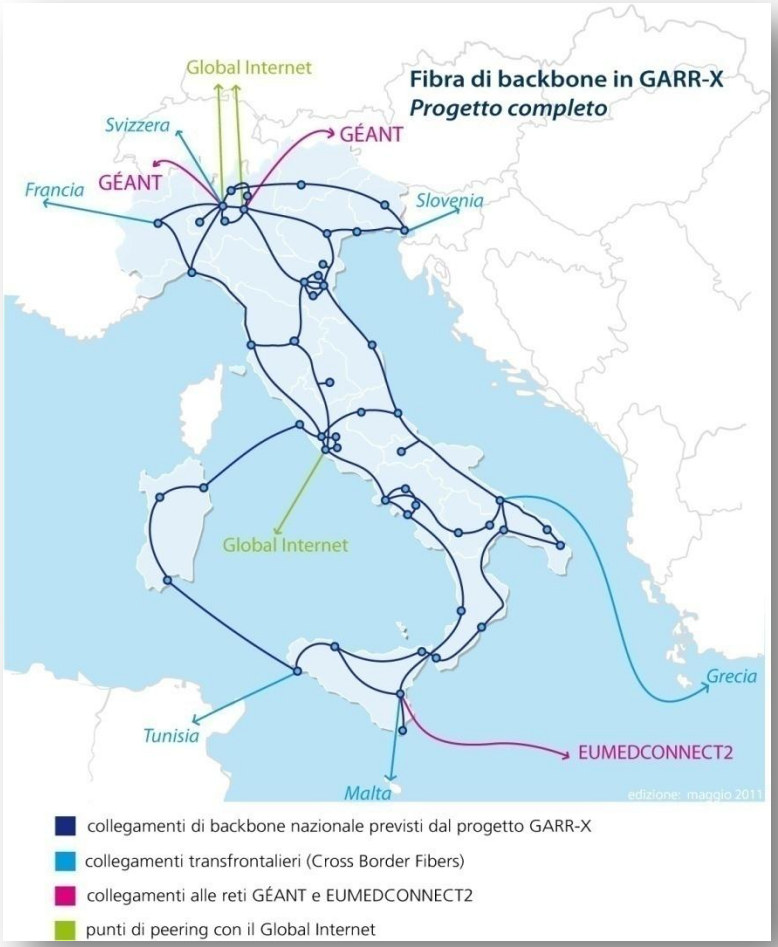


Internet Infrastructure



The Hierarchical infrastructure of internet:
- Tier 1: Full mesh network
- Tier 2: National Internet providers
- Tier 3: Local Internet Service Providers

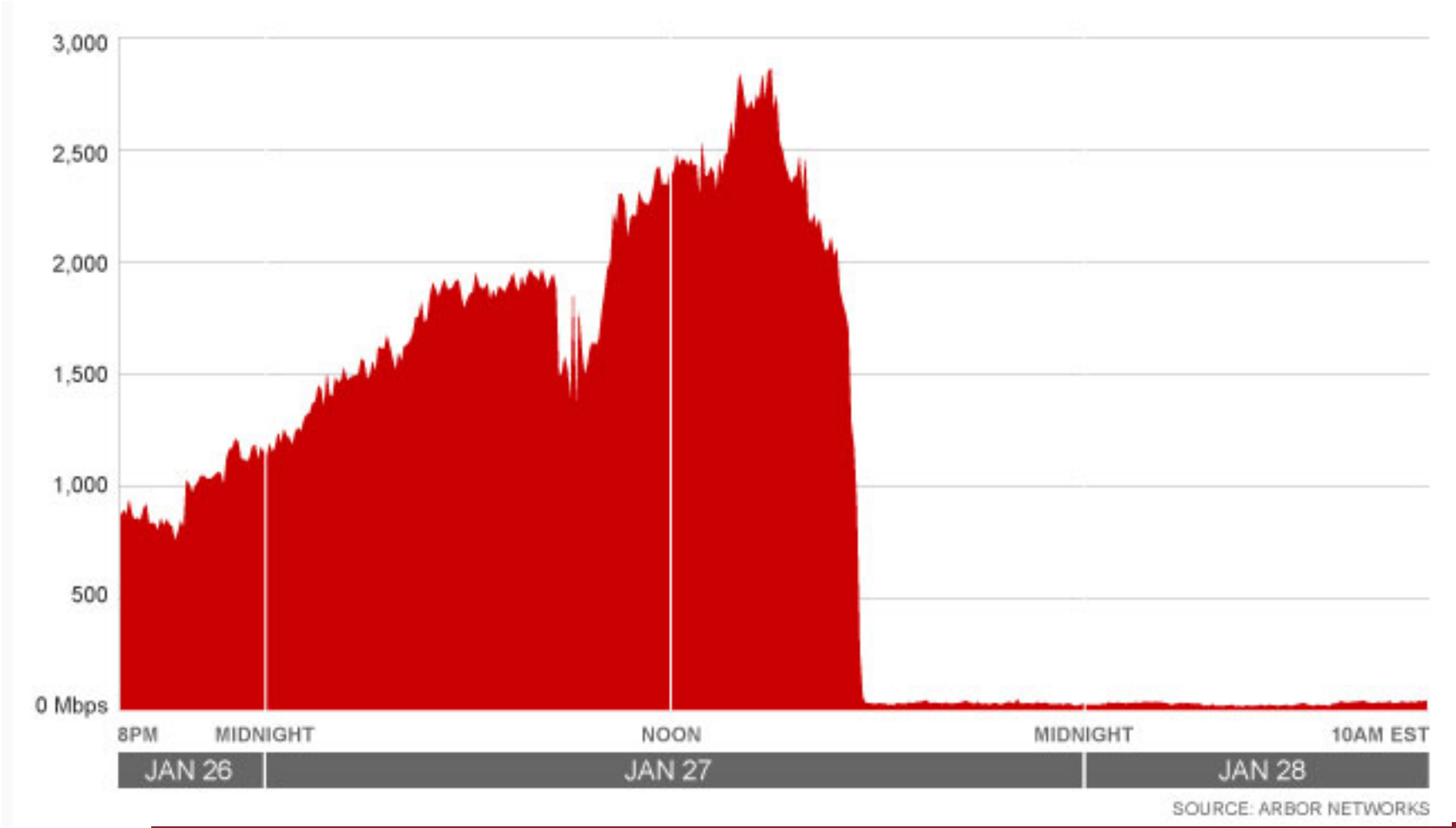
Example Italian Infrastructure



What if the victim resource is the internet connectivity of a whole Member State?

2011: protests in North Africa

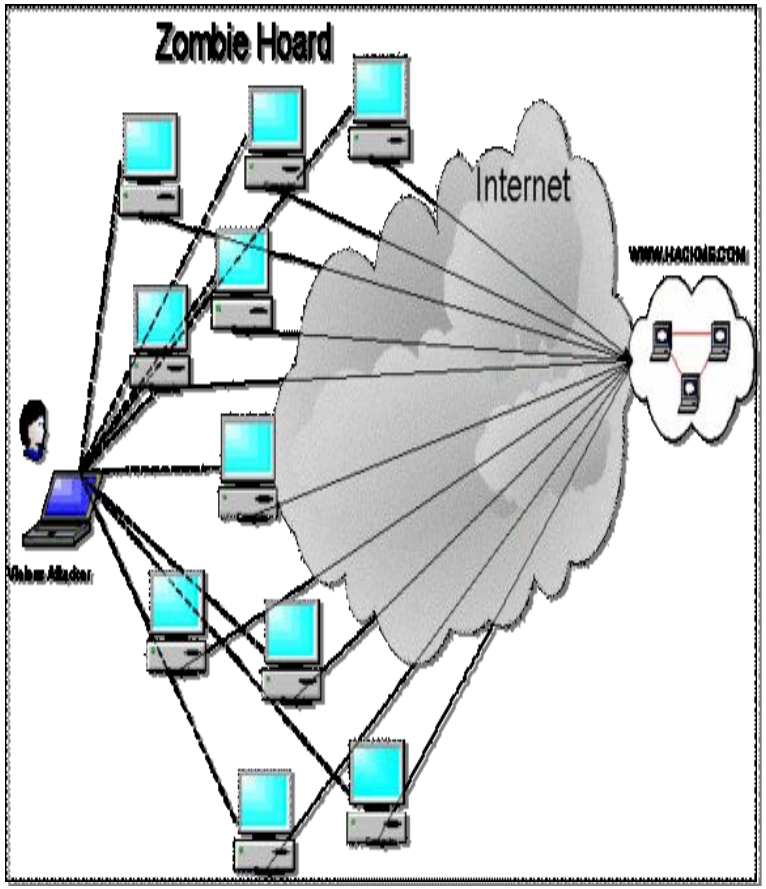
Regimes fight back!



A challenge

To ensure the Nation the capability of secure communication in spite of an untrusted Internet infrastructure

Traditional DDoS Attacks



- Attempt to make a resource unavailable to legitimate users
- Financial and Political hacktivism

Recent (D)DOS attacks (1/3)

"**Mastercard International.** The stock close on 6th Dec 2010 at **$253.60**; Then, on 8th Dec 2010, after news broke that WikiLeak hacker was bombarding the site with requests, the stock dropped to **$246.18** …"

		ime
		-06
		-07
		-07
Joseph Lieberman	lieberman.senate.gov	2010-12-08
MasterCard	mastercard.com	2010-12-08
Borgstrom and Bodström	advbyra.se	2010-12-08
Visa	visa.com	2010-12-08
Sarah Palin	sarahpac.com	2010-12-08
PayPal	thepaypalblog.com	2010-12-09
Amazon	amazon.com	2010-12-09 (Aborted)
PayPal	api.paypal.com:443	2010-12-10
MoneyBookers	moneybookers.com	2010-12-10
Conservatives4Palin	conservatives4palin.com	2010-12-10

Recent attacks (2/3)

- **Sony PlayStation Network**
  - Theft of millions of Credit Card numbers
  - Violations of users' privacy

  (http://www.wired.com/gamelife/2011/04/playstation-network-hacked/)

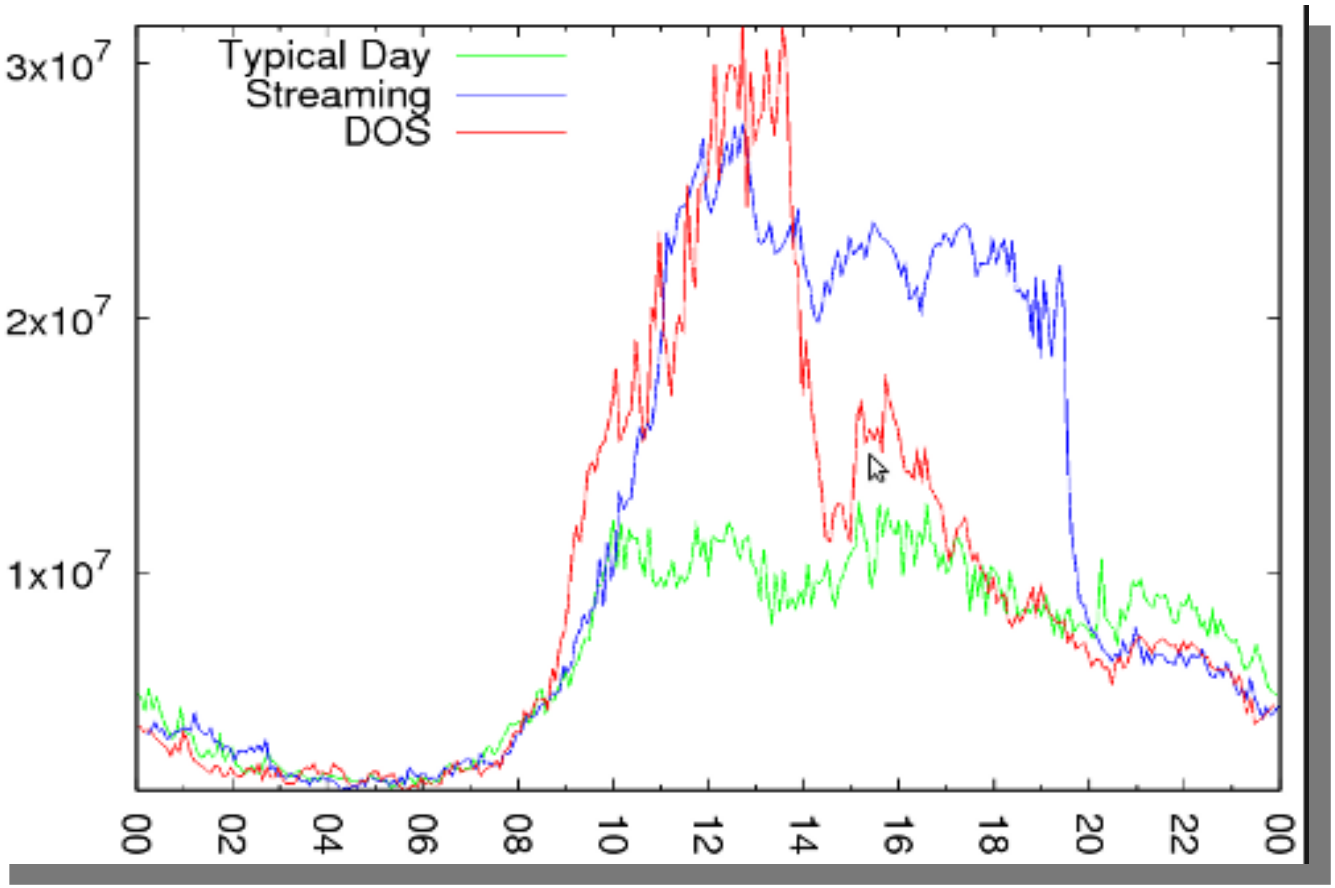
"…hackers now have access to customers' vital information…"

Recent (D)DOS attacks (3/3)

- **Italian Government and house of Representatives**
  - Service disruption
  - Hacktivism
  - Political implications

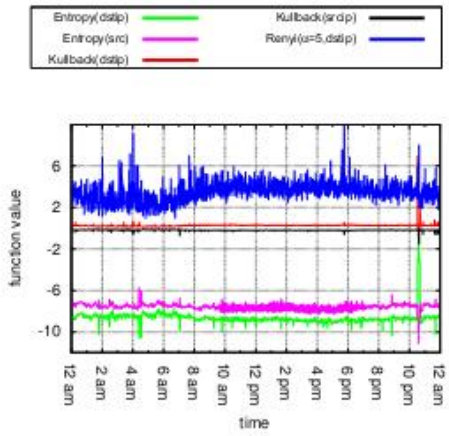
  (http://ansa.it/web/notizie/collection/rubriche_cronaca/02/13/visualizza_new.html_1588579791.html)

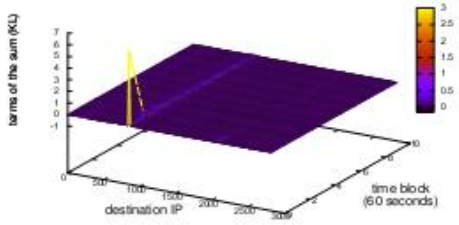
Challenge: early DDoS detection

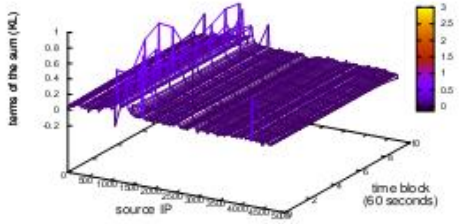


Our results (Secrypt 2012)

DDoS: Metrics comparison and Kullback-Leibler details







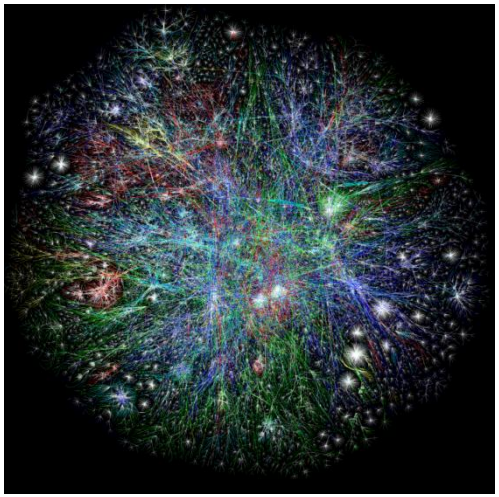
BGP security

Some security issues:

- Control Plane: Does BGP peer correctly performs BGP protocol?
- Data plane: Does IP packets cross the right BGP defined path?

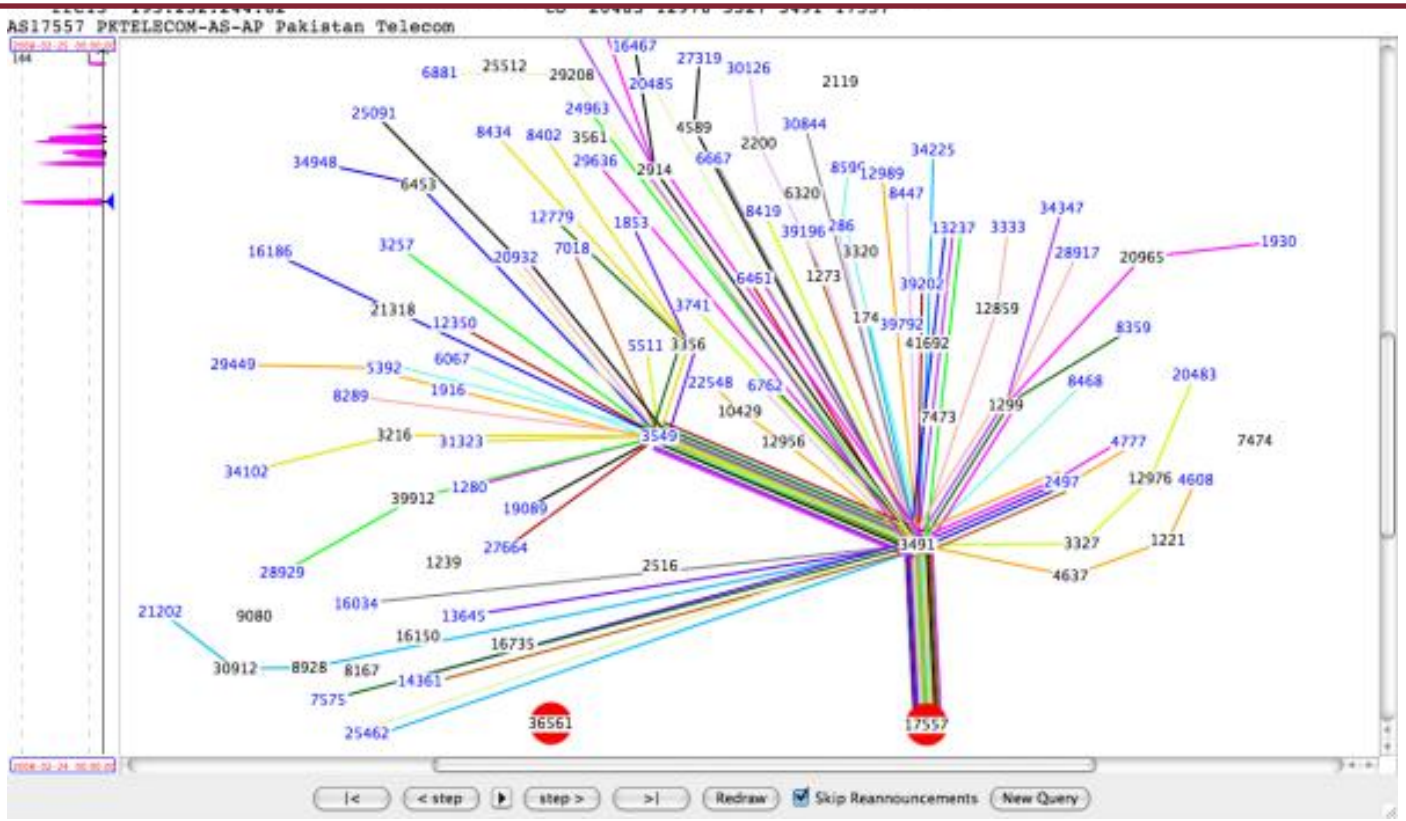
Attack effects

- black hole
- packet drop
- route hijacking



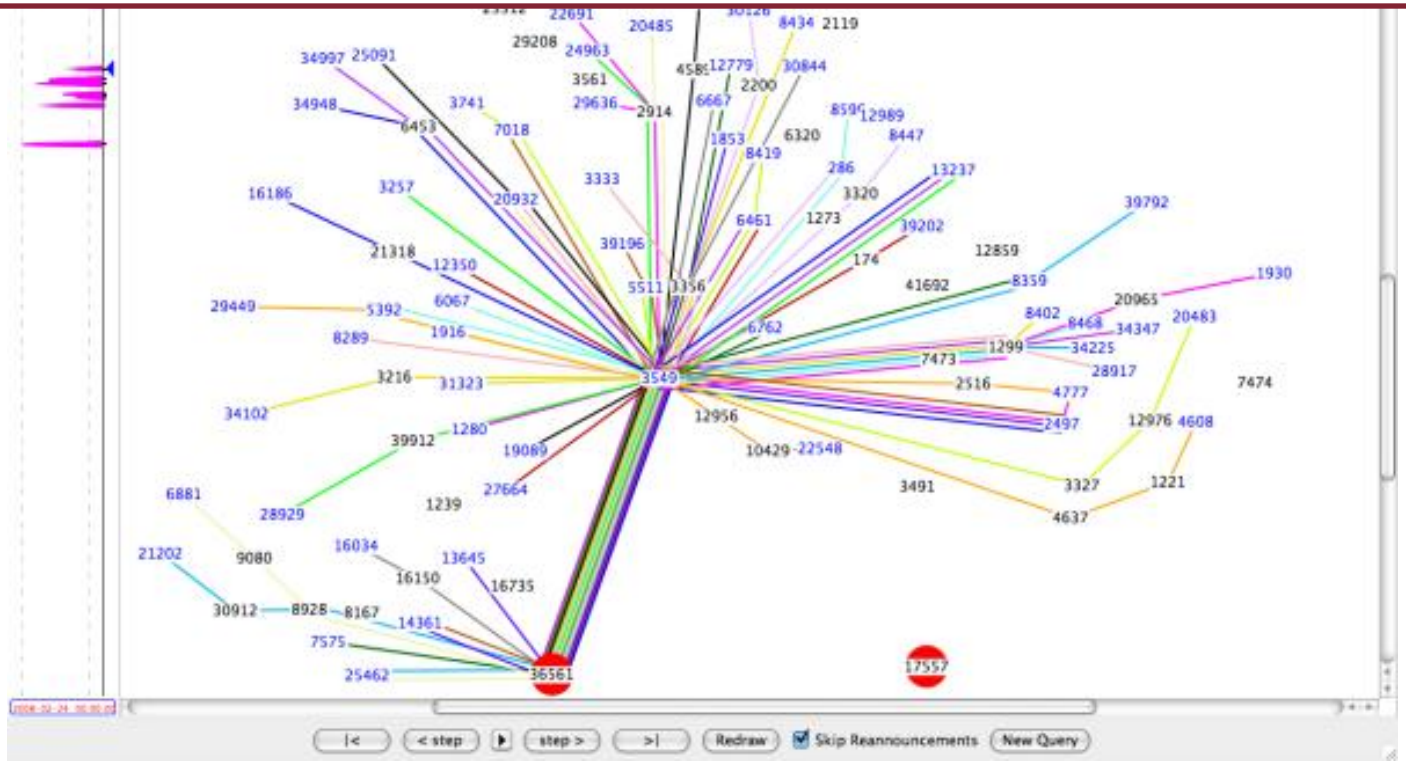
Pakistan Youtube Hijacking

Sunday, 24 February 2008, 18:49 (UTC)
AS17557 (Pakistan Telecom) has been announcing 208.65.153.0/24 for the past two minutes



Pakistan Youtube Hijacking

Sunday, 24 February 2008, 21:23 (UTC)
AS36561 (YouTube) has been announcing 208.65.153.0/24 since 20:07 (UTC). The bogus announcement from AS17557 (Pakistan Telecom) has been withdrawn, and RIS peers now only have routes to YouTube's AS36561



BGP attacks

Recent sensational attacks

- 2010, Chinese ISP hijacked US .gov and .mil web domain: 15% of the world's internet destinations was diverted through China.
- 2008, Pakistan Telecom (AS17557) hijacked some Youtube prefixes (AS36561) due an “unintentional” router misconfiguration

Other examples:

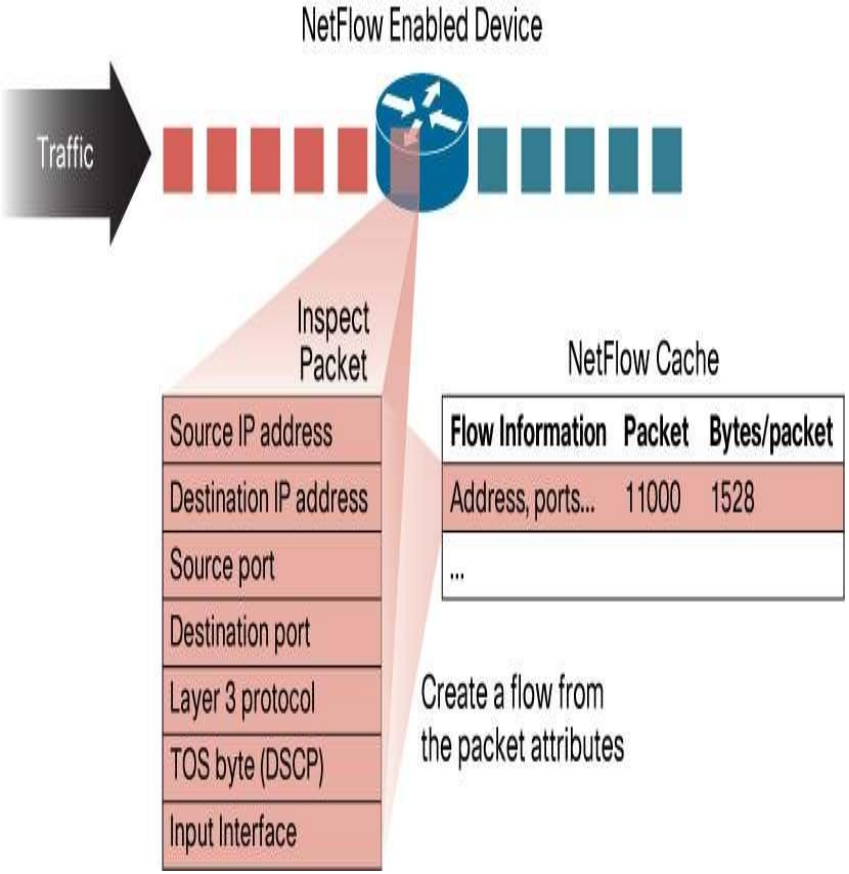
- 2006: Con-Edison hijacked a big chunk of the Internet
- 2004: TTNet in Turkey hijacks part the Internet

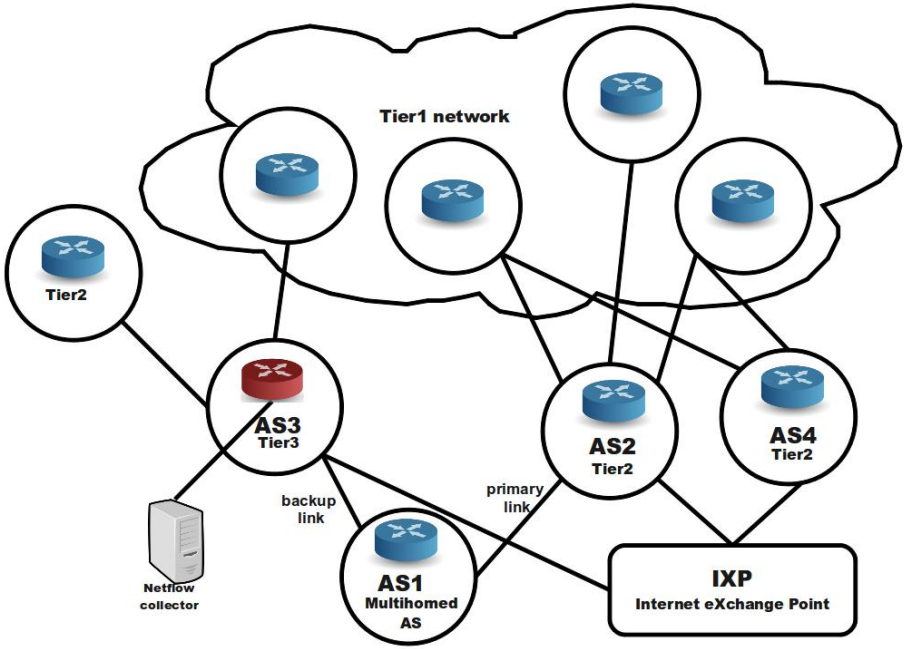
Our proposal (ICCCN 2012)

NO online PKI but use Identity Base Encryption

- I.B.E signature for validating ASPath
- Aggregated signature
- ASPath revocation and AS management (accumulator, witnesses)
- BGP v4 compliant implementation based on OpenBGPd driver (OpenBSD)
- **2012 International Conference on Computer Communication Networks, Munich,Germany**

Network flows Obfuscation





Large set (2 year) of network flows gathered from BGP router of Commercial and Institutional Internet Service Provider.
Dataset expressiveness: 2 GBytes of full netflow entries contain 220 millions of flows, 4 billions of packets corresponding to 5TByte of exchanged data

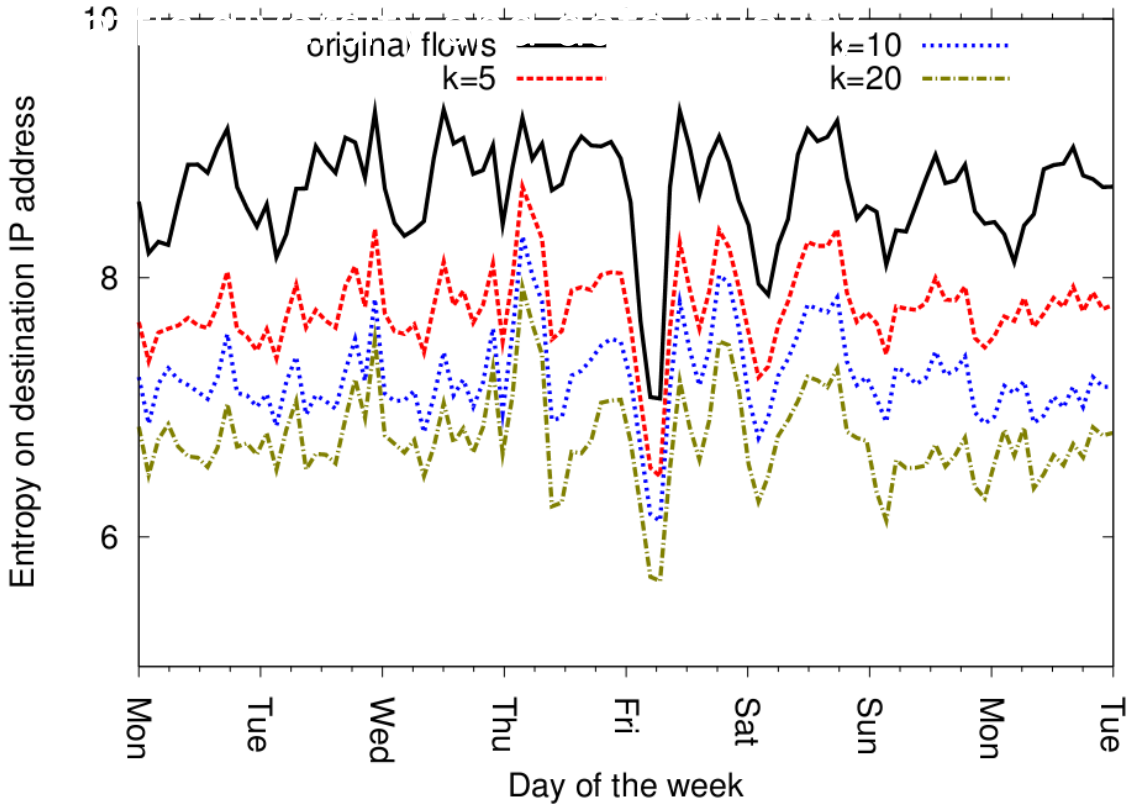
Network Flows Obfuscation

Previous approaches provide encryption of identity fields (IP address) and different techniques on quantitative fields (e.g. TCP flags, traffic stats, etc.):

- Permutation
- Truncation
- Generalization

No formal proof of the obfuscation property of the solution proposed are provided!

K-J Obfuscation (INFOCOM 2012)



Conclusion

- Relevance of the information security governance
- Critical infrastructure and citizen service protection
- To share real attack data, while protecting valuable information (obfuscation, anonymization, etc.)
- Certifications and standards

The final Conference of the ExTrABIRE Project

DIPARTIMENTO
DI INFORMATICA

SAPIENZA
UNIVERSITÀ DI ROMA

CASPUR
CONSORZIO INTERUNIVERSITARIO

Aula Odeion – Museo dell'Arte Classica, Facoltà di Lettere
Università degli Studi di Roma "La Sapienza"
P.le Aldo Moro, 5 – Roma, Italy
Lunedì 18 giugno 2012
Registrazione Ore 9.00