Failures in the current Internet

“Network Resilience” PhD Course, Sep. 26-28th 2011

Failures in the current Internet

1. Topology Failures
2. Overload
3. Lack of Integrity
4. Software Faults
5. Domino Effects

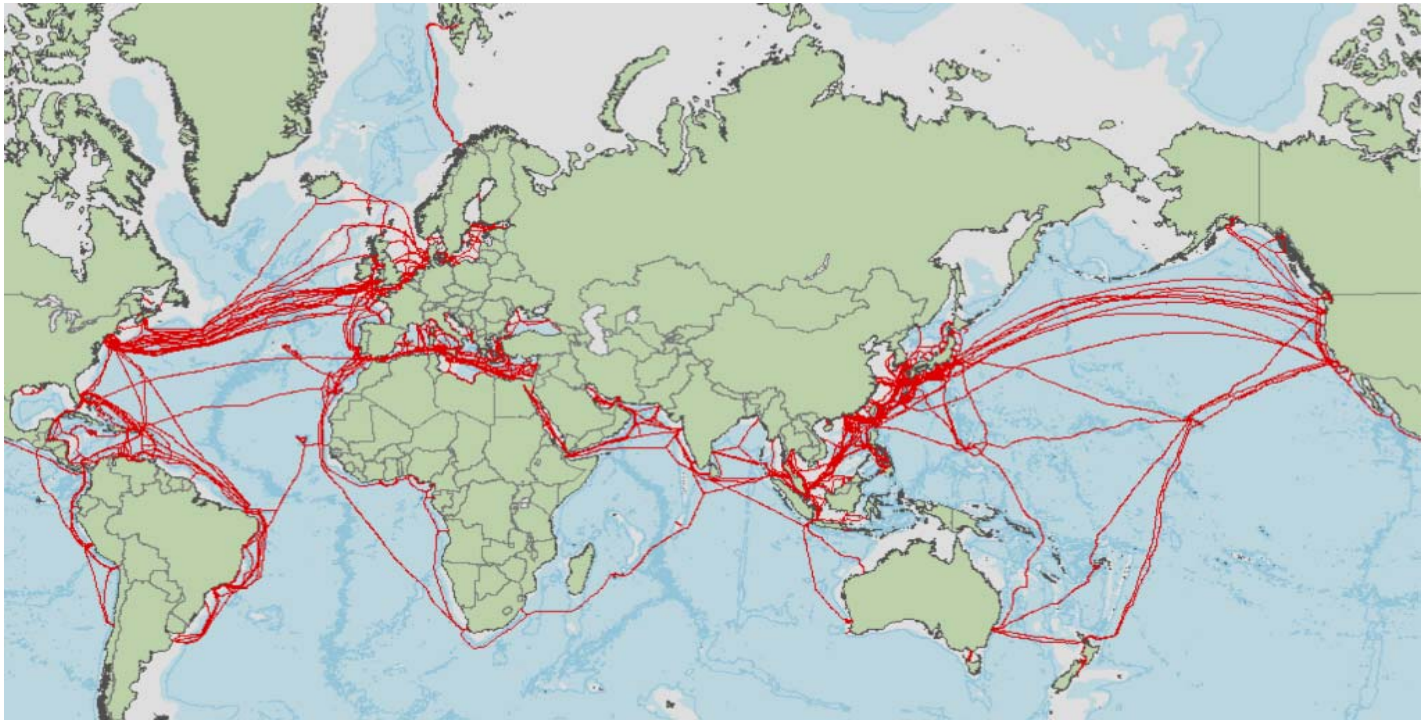
Failures in the current Internet

1. Topology Failures
2. Overload
3. Lack of Integrity
4. Software Faults
5. Domino Effects

Topology Failures

- Failures in the “network graph”
- Network graph
  - Physical topology
  - Logical topology including service dependencies, e.g., DNS
    - ☞ *Dependency graphs*

Topology Failures; Sub-Marine Cables



- ~99% of inter-continental Internet traffic (less than 1% using satellites)
- High redundant
- But vulnerable to
  - Fishing and anchoring (70% of sub-marine cable failures)
  - Natural disasters (12%)
  - Cable theft

Submarine Cables; Natural Disasters

- Hengchun earthquake (December 2006)

Bloomberg.com

BloombergAnywhere

Updated: New York, Oct 27 1

QUOTE SEARCH NEWS SYMBOL LOOKUP Live TV

HOME NEWS MARKET DATA PERSONAL FINANCE TV and RADIO

news

Technology Currencies Forex Trading Videos ETFs CEO Commodi

- Exclusive
- Worldwide
- Regions
- Markets
- Industries
- Economy
- Politics
- Law
- Environment
- Science
- Opinion
- Spend

Asian Internet, Phone Services Hit by Taiwan Quakes (Update2)

Share | Email | Print | A A A

By Tim Culpan and Andrea Tan

Dec. 27 (Bloomberg) -- Internet and telephone services across Asia were disrupted, hampering financial transactions, after earthquakes near Taiwan damaged undersea cables.

``The repairs could take two to three weeks,'' said Leng Tai-feng, president of Chunghwa Telecom Co.'s international business. The Taipei-based company, Taiwan's largest phone operator, said two of its undersea cables were cut.

Submarine Cables; Natural Disasters

- Hengchun earthquake (December 2006)
- Impact
  - Affected countries: China, Taiwan, Hong Kong, Philippines
  - China‘s Internet connectivity reduced by 70%
  - Hong Kong‘s Internet access completely disabled
- Recovery
  - BGP automatic re-routing helped to reduce disconnectivity
  - But resulted into congested links
  - Manual BGP policy changes + switch port re-configuration were necessary
  - Hong Kong‘s Internet users were still experiencing slow Internet connections 5 days after the earthquake

Submarine Cables; Failures in the Mediterranean Sea

- In Jan. + Feb. 2008, 3 successive events

- Impact
  - Affected countries: Egypt, Iran, India and a number of other middle east countries
  - Disruption of
    - 70% in Egypt
    - 60% in India

Submarine Cables; Cable Theft

- In March 2007, pirates stole an 11 kilometers section of the submarine cable connecting Thailand, Vietnam and Hong Kong,
- Impact: significant downgrade in Internet speed in Vietnam.
- Intention: The thieves wanted to sell 100 tons of cable as scrap.

Topology Failures; Routing

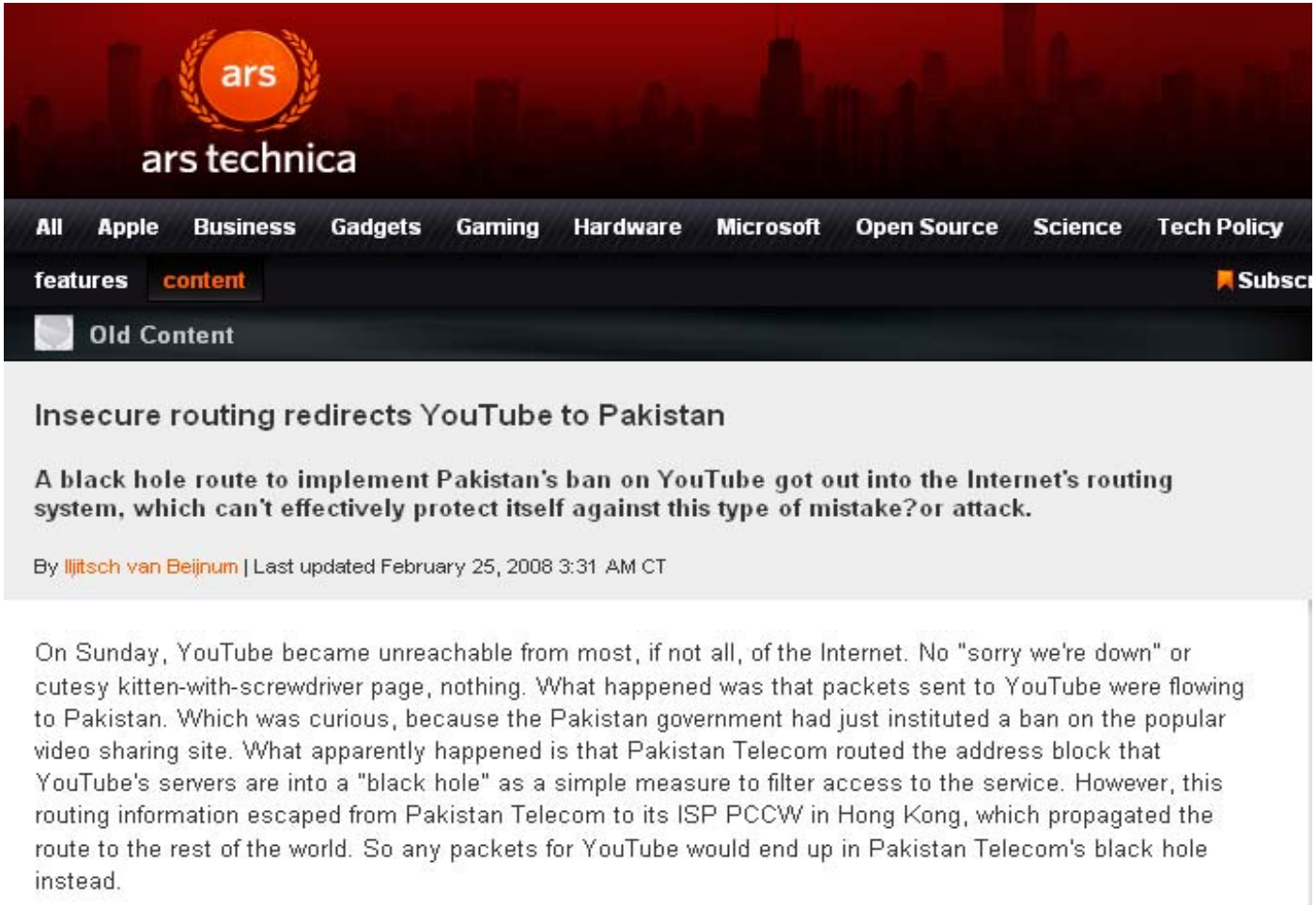
- Failures in the IP topology graph
  - Failures of routers (nodes)
  - Failure of links between routers
- Failure of links between routers generally caused by disconnection at lower layers
- Failure of routers
  - DoS attacks
  - Failures due to software bugs
  - Examples of reported bugs
    - Vulnerability to too long AS (BGP Autonomous Systems) paths
    - Long passwords to login to the router
    - Overflow of connection tables in some commercial firewalls

Topological Failures; Routing

- Time to Recovery
  - Intra-domain routing (OSPF, RIP, IS-IS, EIGRP): up to several 100ms
  - Inter-domain routing (BGP): up to several minutes

Topological Failures; Routing

- Other reasons
  - Misconfiguration which leads to false modification of the Internet topology



Failures in the current Internet

1. Topology Failures
2. Overload
3. Lack of Integrity
4. Software Faults
5. Domino Effects

Overload

- Topology failures are binary (link or node is up or down)
- But equipment in the network (routers, servers, etc.) have limited capacity
  - Queue length
  - CPU power
  - etc.

☞ Overload (congestion) is not rare

Lack of Congestion at the Network Layer

- Routing protocols react to the failure of a link or a router.
- But not to network congestions
- ARPANET had some mechanisms to react to congestions
- But they resulted into oscillations
- Congestion control was introduced in the Internet as enhancement of TCP
- But TCP has
  - no knowledge about the network topology
  - no way of re-wiring the traffic path in case of congestion

DoS Attack vs. Flash Crowds

- Big challenge
  - Ambiguous differentiation between DoS attacks and *flash crowds*
  - *Flash crowds*: unusual but legitimate traffic
  - Even if attacks are identified as such, it remains difficult to separate between malicious and legitimate traffic and to eliminate the malicious traffic

DoS Attacks

- Some DoS attacks have a political or ethnical reasons

Low graphics | Accessibility help

BBC NEWS

Watch One-Minute World News

News services
Your news when you want it

News Front Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology
Entertainment

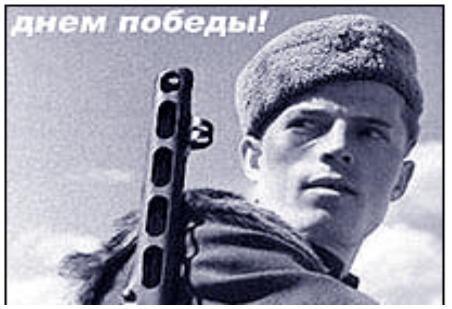
Last Updated: Thursday, 17 May 2007, 14:52 GMT 15:52 UK

E-mail this to a friend Printable version

The cyber raiders hitting Estonia

As Estonia appeals to its Nato and EU partners for help against cyber-attacks it links to Russia, the BBC News website's Patrick Jackson investigates who may be responsible.

Estonia, one of the most internet-savvy states in the European Union, has been under sustained attack from hackers since the ethnic Russian riots sparked in late April by its removal of a Soviet war memorial from Tallinn city centre.



SEE ALSO
- Estonia hit by 'Moscow cyber war' 17 May 07 | Europe
- Hackers attack heart of the net 07 Feb 07 | Technology
- Playing Estonia's political cards 12 May 07 | Europe
- News fuels Russian internet boom 10 Apr 06 | Europe
- Country profile: Estonia 30 Apr 07 | Country profiles

RELATED INTERNET LINKS
- Estonian foreign ministry
- Russian government
- Kaspersky Lab

Failures in the current Internet

1. Topology Failures
2. Overload
3. Lack of Integrity
4. Software Faults
5. Domino Effects

Lack of Integrity

- Majority of Internet traffic (signaling and data) is not integrity-protected
- This leads to several security vulnerabilities
  - ARP poisoning
  - Forged BGP announcements
  - Forged DNS responses
  - SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM
  - etc.

Failures in the current Internet

1. Topology Failures
2. Overload
3. Lack of Integrity
4. Software Faults
5. Domino Effects

Software Faults

- Developments faults
  - Introduced during the development phase
- Configuration faults
  - Introduced during the deployment phase

Software Faults

- Examples
  - Development faults: Lack of bound checking in the code
    - Leads to buffer overflows in server or router implementation
    - Leads to router or server failure
  - BGP Youtube misconfiguration
  - On Jan. 31st 2009, Google search engine marked every search result with "This site may harm your computer";

    Root cause: Database of suspected sites was mistakenly extended by ‚/‘
  - Software update of the Authentication Server (Home Location Register HLR) of T-Mobile on April 21st 2009
    - Impact: phone calls and text messaging were not possible for 4 hours

Failures in the current Internet

1. Topology Failures
2. Overload
3. Lack of Integrity
4. Software Faults
5. Domino Effects (Cascading Failures)

Domino Effects (Cascading Failures)

- Any kind of challenges mentioned above may lead to other challenges
  - E.g., failure of a server in a server pool may lead to overload of neighboring servers
  - Router failures may lead to congestion of neighboring links and routers
  - DNS failure may lead to unavailability of other services,

Domino Effects

- E.g., DoS attack on Microsoft router on 24th + 25th Jan. 2001 lead to unavailability of DNS and thus of services located in other MS sites