Content blocking methods and their impacts

RIPE68 - Warsaw, Poland
RIPE Cooperation Working Group
15 May 2014

Pier Carlo Chiodi
http://pierky.com/aboutme
pierky@pierky.com

Adapted and presented by
O. Kolkman
olaf@NLnetLabs.nl

Presentation Goal

Provide a guide or overview of documents that discuss the impact of various content blocking mechanisms

http://www.pierky.com/docs/ATechnicalOverviewOfContentBlockingMethods.pdf
by Pier Carlo Chiodi (first version)

and
http://tools.ietf.org/html/draft-iab-filtering-considerations
IAB document edited by Barnes, Cooper and Kolkman (6th version)

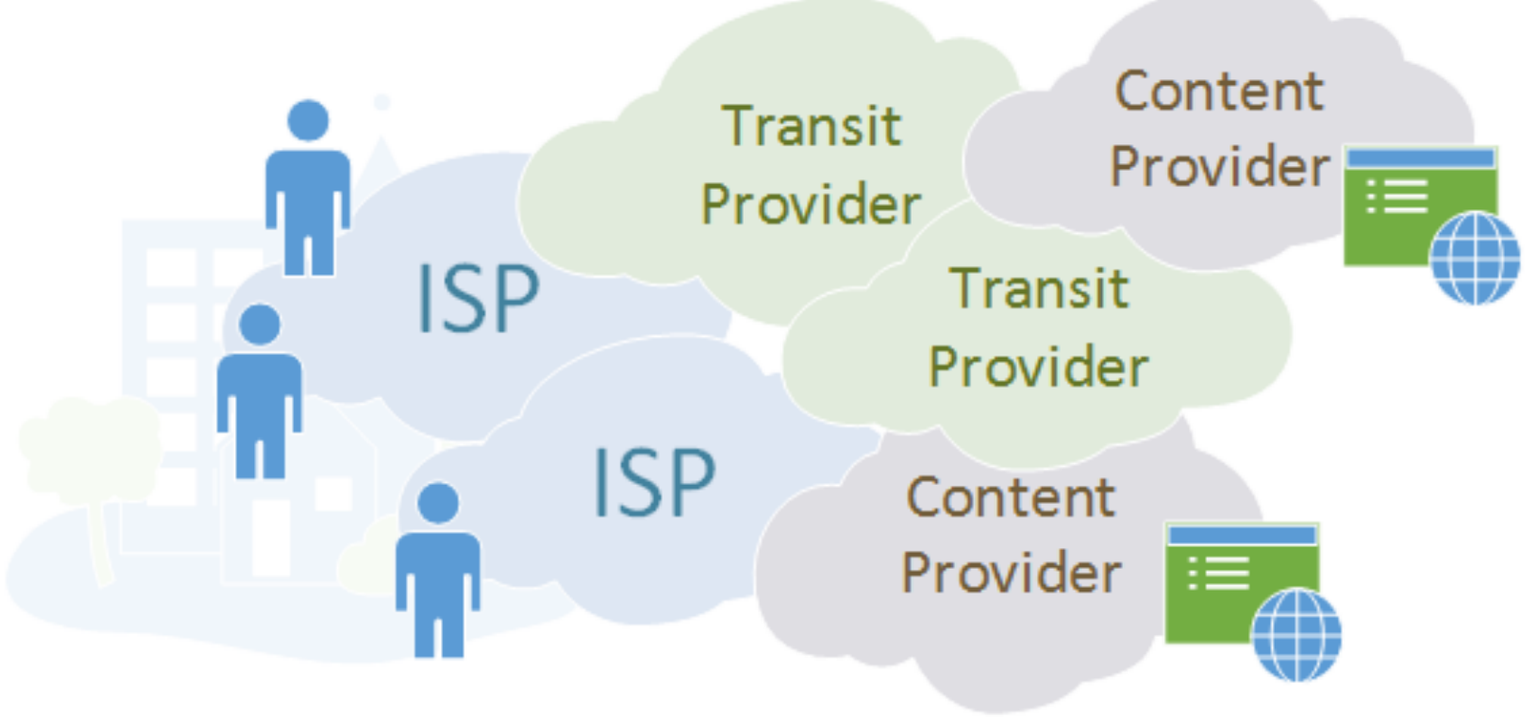
Also see Stephane Bortzmeyer's presentation in the DNS WG and references therein

Summary

- **How Internet works: the life cycle of a web request**
- Content blocking: why, where and how (not)
- Analysis of blocking/filtering methods
- Side effects
- Conclusions
- Q&A

How Internet works: overview

- **Internet Service Providers** (ISPs): allow users to connect their devices to Internet.
- **Content Providers** and **Web Sites Operators**: host web sites, mail boxes, services and media contents on their servers.
- **Transit Providers**: allow other networks to exchange traffic with each other.

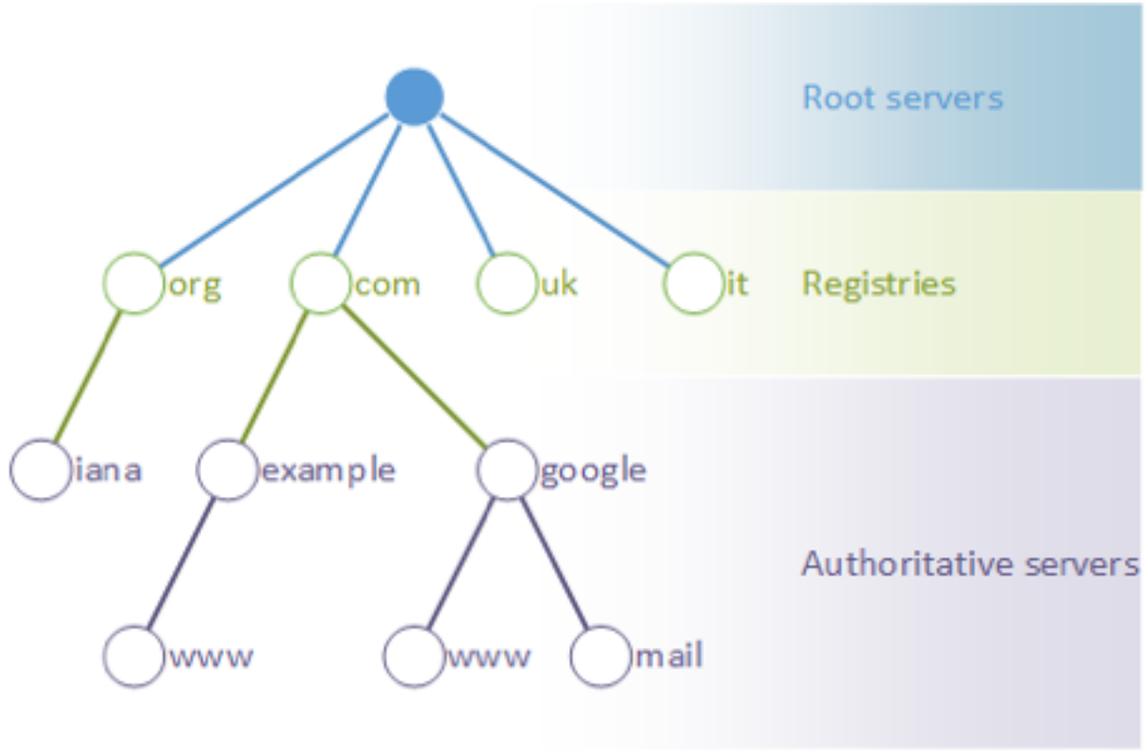


How Internet works: overview

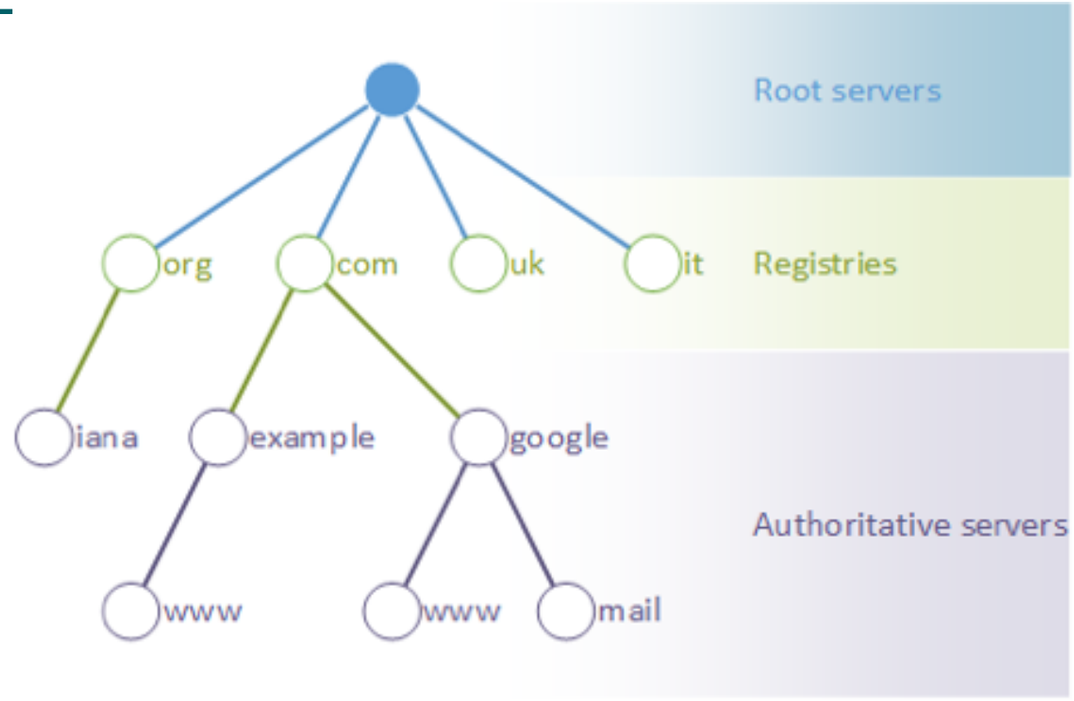
- Devices talk each other by exchanging "**packets**".
- Packets traverse links and networks **from source to destination**.
- They carry commands and instructions to setup a communication between users' devices and servers (**client/server** model).
- Packets are addressed using a numerical identifier, an **IP address** (e.g. 93.184.216.119), which uniquely identifies a device.
- Numbers are hard to remember; **DNS** allows to associate a numerical IP address to a name used to represent a resource (www.example.com instead of 93.184.216.119).

How Internet works: DNS

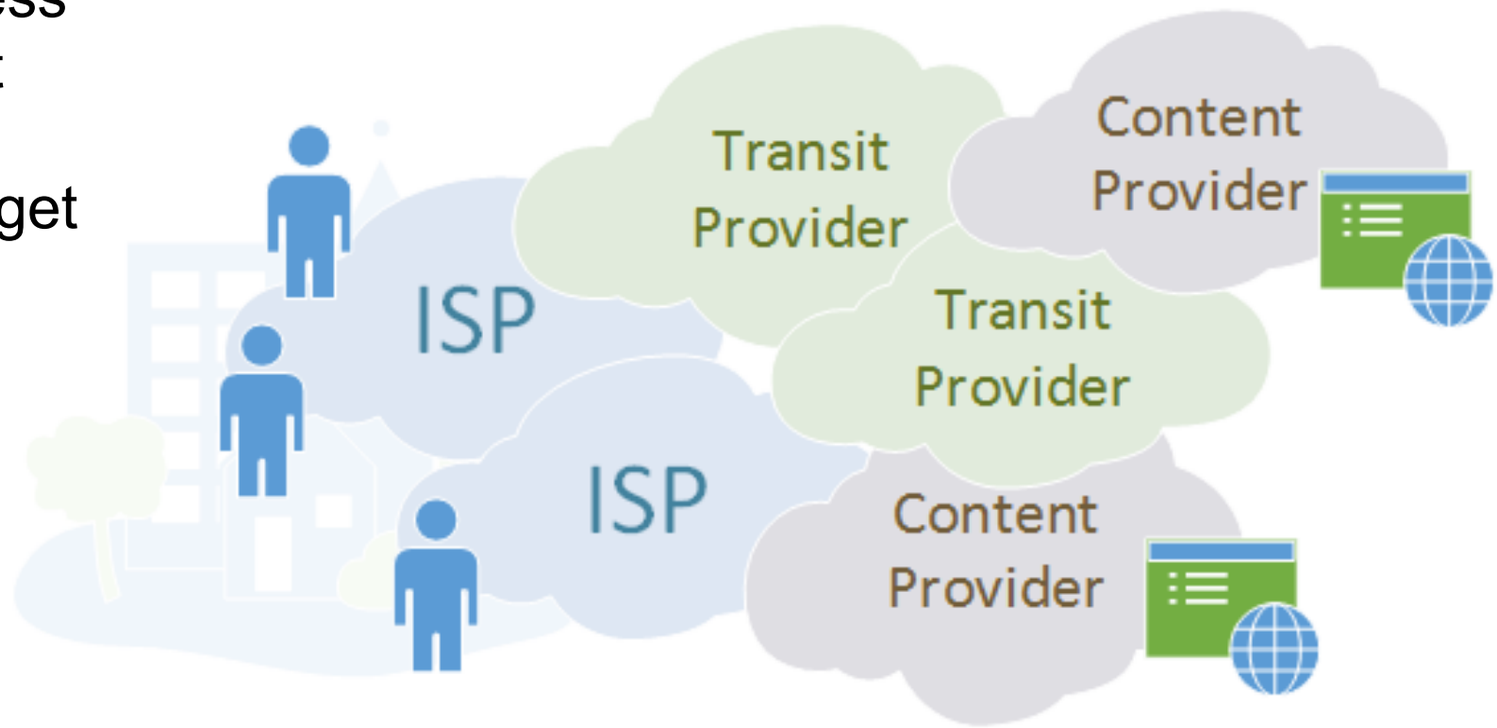
- **Root servers**: list of servers responsible for “Top Level Domains” (TLDs), such as .com, .org, .net.
- **Registries**: list of all the domain names (like example.com) which belong to the TLD zone they have in charge of.
- **Domain authoritative servers**: list of services that each domain offers (e.g. www).
- **Recursive resolvers**: servers provided by ISPs and used by devices to resolve names.



Note that the DNS tree depicts the relation between DNS data managers it doesn't prescribe where all these nodes are located in the network or geo topography.



In order to use an application service a user will first use the Internet to access the DNS to find where in the Internet topology the application service is located and then use the Internet to get to it.



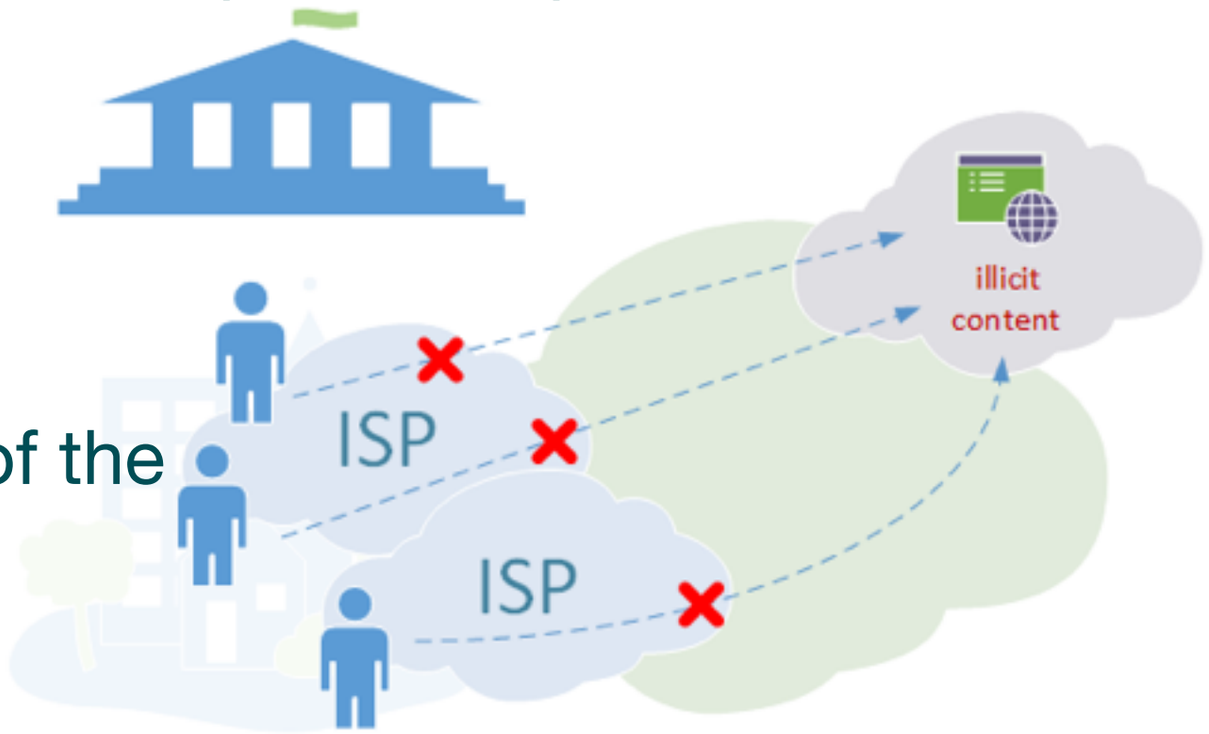
Summary

- How Internet works: the life cycle of a web request
- **Content blocking: why, where and how (not)**
- Analysis of blocking/filtering methods
- Side effects
- Conclusions
- Q&A

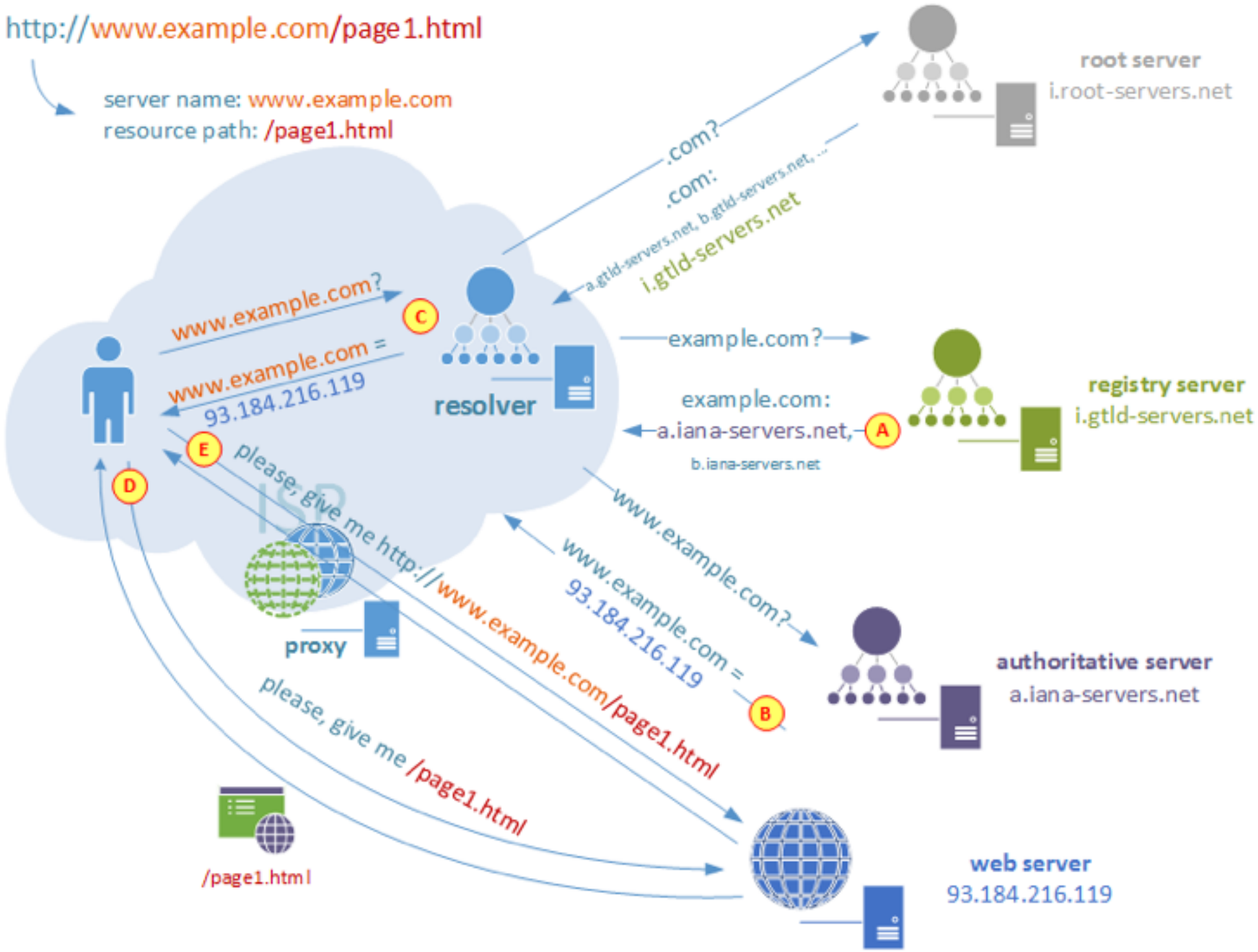
Why do folk turn to content blocking

- To prevent access to **illegal contents** (child abuse, unauthorized gaming and gambling, piracy) or **illicit (taboo) content** (pornography, gaming and gambling)
- To constrain access to **opposing political or religious** contents.
- To **quiet debates** that threaten the parties in power.

Used when contents or services are hosted on servers out of the **jurisdiction** of the requesting party.



Content blocking: control points



Content blocking: collateral damage

- **Overblocking**

  Prevent a content to be accessed by blocking a whole IP/domain (e.g. prevent access to a blog post by filtering out the whole blog platform).

- **DNSSEC breakage**

  DNSSEC fights fake DNS responses to avoid traffic hijacking, but some content blocking measures just use injected false responses to block resources. Risks: impairment of trust on this technology and delay in its adoption.

Summary

- How Internet works: the life cycle of a web request
- Content blocking: why, where and how (not)
- **Analysis of blocking/filtering methods**
- Side effects
- Conclusions
- Q&A

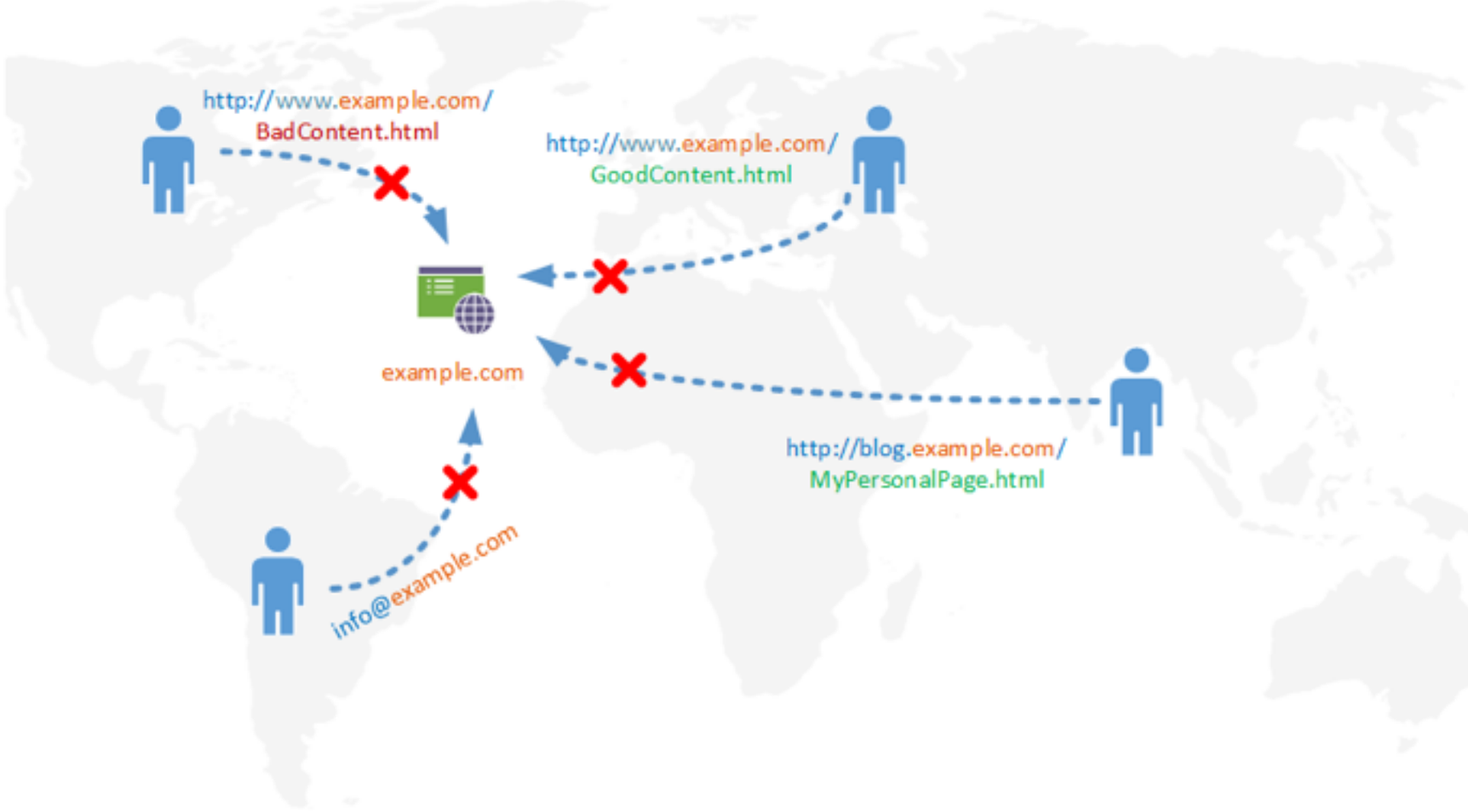
Analysis of blocking/filtering methods

- **Scope**: to evaluate which users are blocked.
- **Granularity**: to evaluate how specific is the blockage/filter and its impacts on other services and contents.
- **Efficacy**: to evaluate how difficult it is for users to avoid the blocking measure.
- **Security**: to evaluate impacts of the blocking measure on the security of Internet (availability, authenticity, confidentiality and integrity).
- **Feasibility**: to evaluate difficulties and costs related to the implementation of the method.

Method A: DNS Registries

Removal of a domain name from a Registry (domain take-down).

- **Scope**: the whole Internet with disregard of jurisdictional borders.
- **Granularity**: any service of that domain impacted.



Method A: DNS Registries

- **Efficacy**: contents still accessible by IP or little change on devices configurations.
- **Security**: compatible with DNSSEC provided that the Registry would also remove any DNSSEC configuration.
- **Feasibility**: the Registry which holds the domain may be out of the jurisdiction of the requesting party. Very low technical costs.

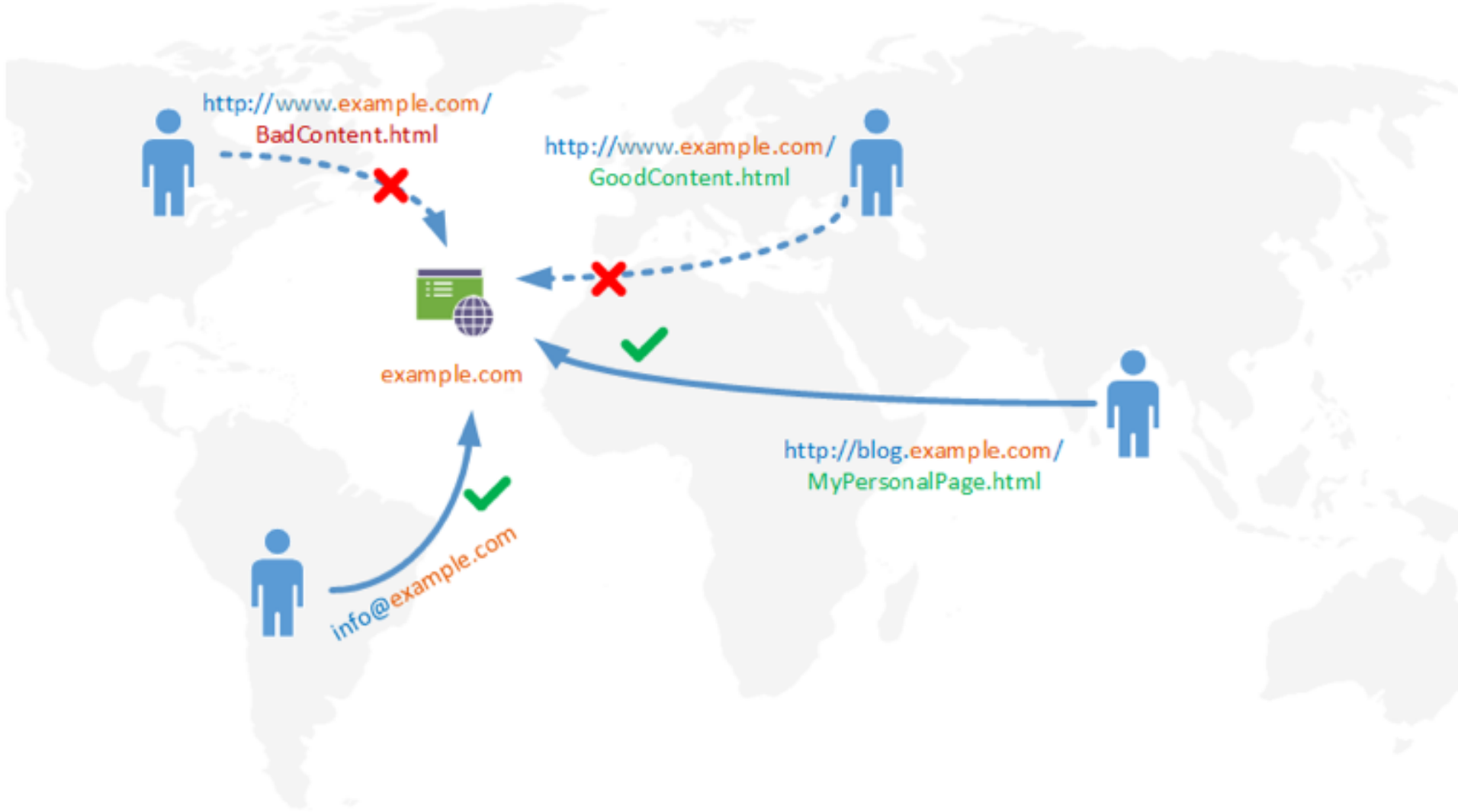
Method B: Domain Authoritative Servers

Takedown notice sent to who is in charge of the target domain zone.

- **Scope**: global impact only if implemented on all the Authoritative servers that handle the domain name.

Method B: Domain Authoritative Servers

- **Granularity**: only services impacted by the blocking request (e.g. www down while email still working).



Method B: Domain Authoritative Servers

- **Efficacy**: contents still accessible by IP or little change on devices configurations.
- **Security**: in most cases DNSSEC capable devices would consider any response from the Authoritative server as not valid.
- **Feasibility**: every authoritative name-servers must be reconfigured to achieve global blockade. Minimal technical costs.

Method C: ISP DNS Recursive Resolvers

Requestors order ISPs to block a domain on their resolvers.

- **Scope**: only users within jurisdictional borders of the requestors are impacted. Every national ISP must be contacted, otherwise a non-homogeneous and discriminatory treatment would be reserved to people.

Method C: ISP DNS Recursive Resolvers

- **Granularity**: high overblocking risk like every DNS-based blockade.
- **Efficacy**: out-of-border free DNS services (e.g. Google, OpenDNS) allow to easily bypass the blockades. Contents still accessible by IP or little change on devices configurations.

Method C: ISP DNS Recursive Resolvers

- **Efficacy**: out-of-border free DNS services (e.g. Google, OpenDNS) allow to easily bypass the blockades. Contents still accessible by IP or little change on devices configurations.

Source http://www.renesys.com/wp-content/uploads/2014/03/twitter-turkey-googledns.jpg

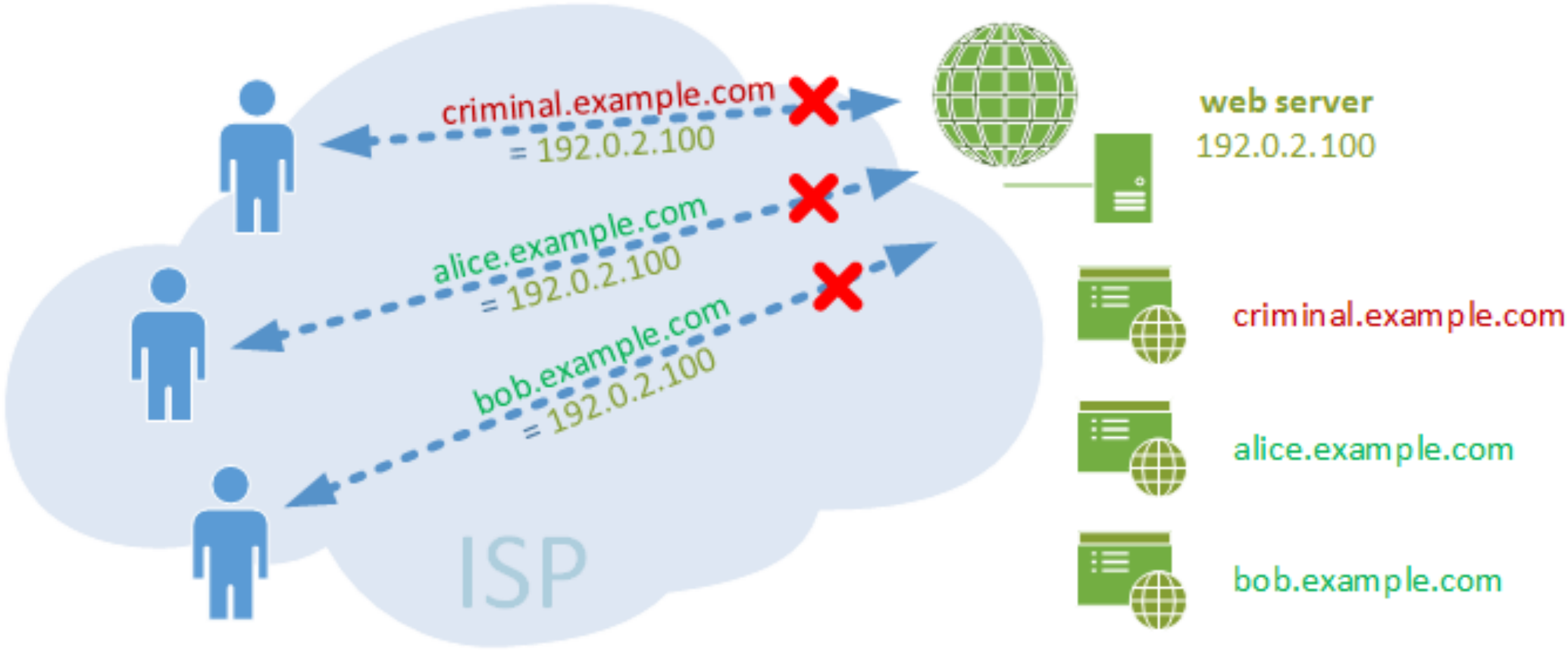
Method C: ISP DNS Recursive Resolvers

- **Security**: DNSSEC is highly impacted; some responses may be interpreted by clients as a server malfunctioning and lead operating systems to remove it from the list of those to be used.
- **Feasibility**: no governments cooperation is required; costs and technical requirements are negligible.

Method D: ISP IP address block

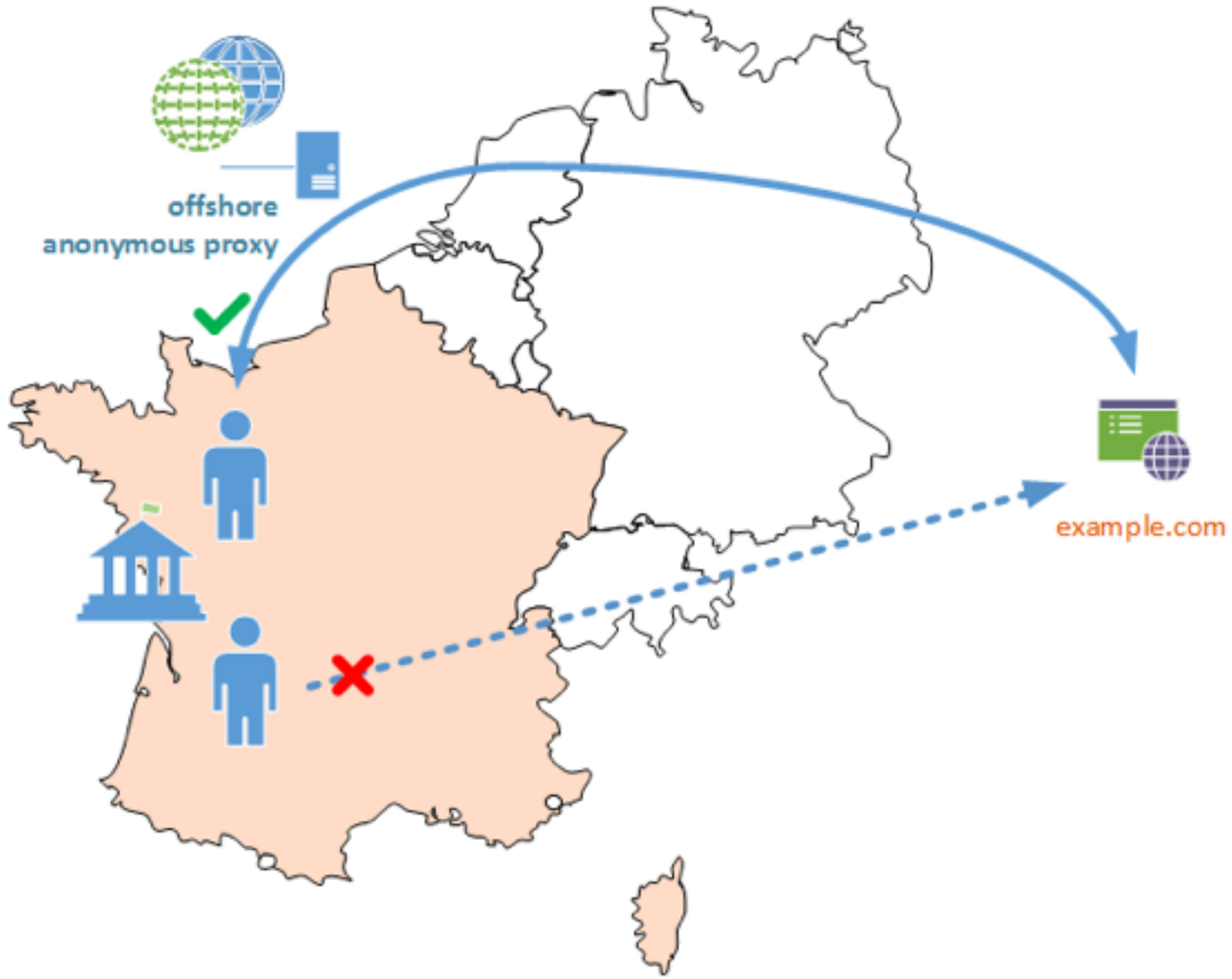
Requestors order ISPs to block an IP address on their network.

- **Scope**: only ISPs and customers within borders are involved.
- **Granularity**: highest possible impact on contents and services.



Method D: ISP IP address block

- **Efficacy**: users may route their traffic away from the blocking enforcement using VPN and proxies.
- **Security**: DNSSEC is not impacted, but many side effects exist.



Method E: ISP Web Proxies and DPI

Requestors order ISPs to filter web requests from their customers (web-proxies) or to monitor content of every packet on their network (DPI, Deep Packet Inspection) and block those that matches a specific pattern.

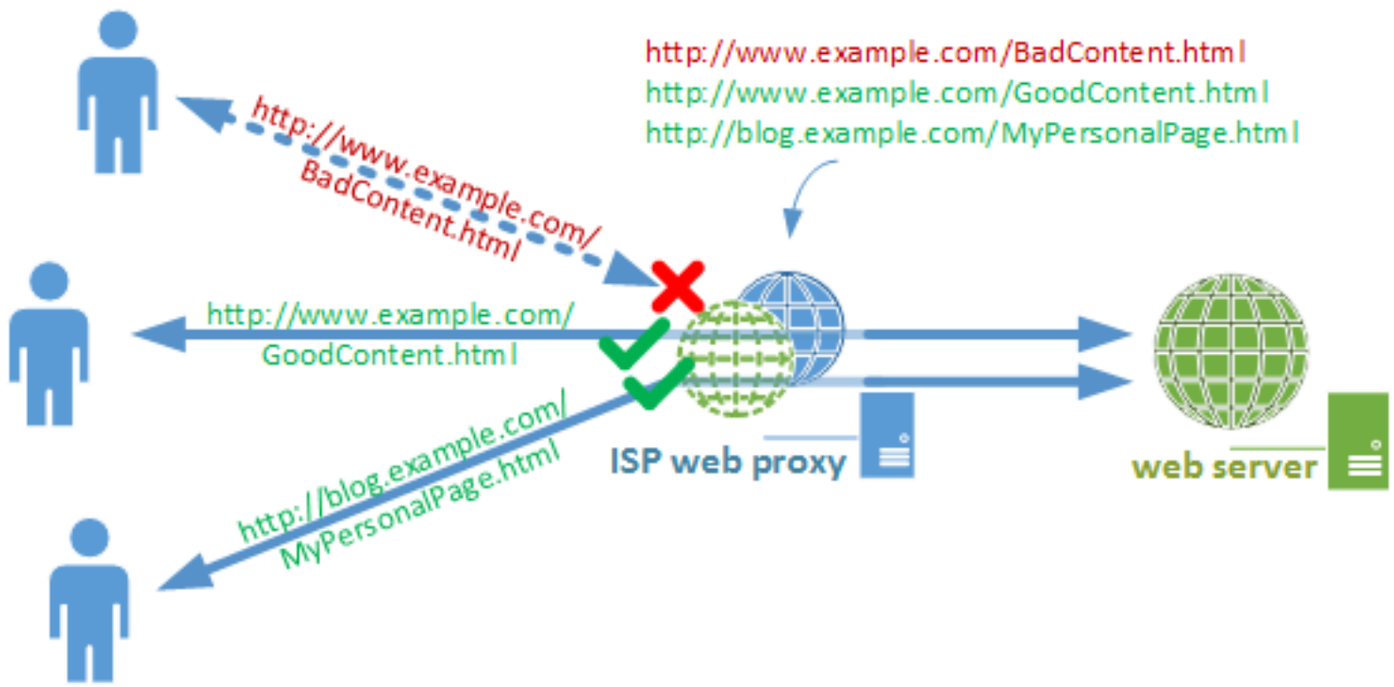
- **Scope**: only customers within the same jurisdiction of the requestor are involved.

Method E: ISP Web Proxies and DPI

- **Granularity**: methods with the finest granularity.

  Any content request is diverted to a web proxy or to a DPI station which analyzes it and then decides to handle it or to drop it.

  Proxies only work for web contents (HTTP, HTTPS), while DPI allows to classify (and eventually block) any protocols.



Method E: ISP Web Proxies and DPI

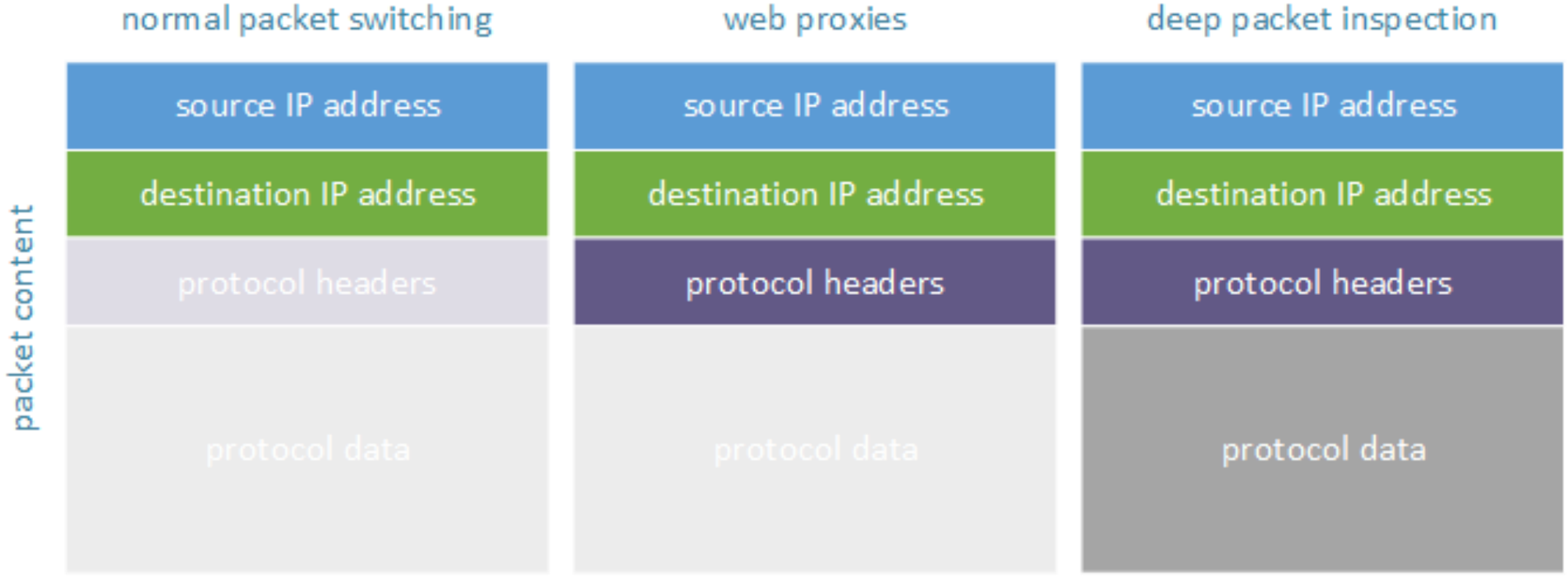
- **Efficacy**: blocking enforcements and DPI stations must be placed by ISPs along their network in order to block and intercept all customers traffic. Efficacy is closely bound up with obfuscation and encryption techniques which are over and over improved. VPNs may be used to bypass proxies.

Method E: ISP Web Proxies and DPI

- **Security**: secure encrypted web connections (HTTPS) are broken by proxies, introducing a security weakness on paths that users consider fully trusted. New protocols aimed to detect third-party entities along those paths may lead modern browsers to block any communication with the target web server.

Method E: ISP Web Proxies and DPI

- **Feasibility**: these methods don't require governments cooperation. Costs and difficulties are very high: additional hardware and software must be deployed, solutions are expensive and require big maintenance efforts.



Summary

- How Internet works: the life cycle of a web request
- Content blocking: why, where and how (not)
- Analysis of blocking/filtering methods
- **Side effects**
- Conclusions
- Q&A

Side effects

If users know that the contents they want to access are still online but to access them something has to be changed on their devices, it is likely that these changes develop quickly on large scale.

These behaviors, which all lead to exposure of users to threats, are expected to grow with the growth of the number of (over-)blocked resources.

Side effects

- **Extended trust on automatic configuration script**: inexpert users trust automatic configuration script provided by web sites operators and let them to change devices configuration.
- **Use of untrusted resolvers and proxies**: every users' Internet activity crosses untrusted servers.
- **Defeat of anti-cybercrime activities**: local anti-cybercrime activity vanished by the usage of open resolvers.
- **Impacts on Content delivery networks**: contents tuned on the basis of DNS responses have their performances impacted.

Summary

- How Internet works: the life cycle of a web request
- Content blocking: why, where and how (not)
- Analysis of blocking/filtering methods
- Side effects
- **Conclusions**
- Q&A

Conclusions

- ISP-focused enforcements have a closer scope than other.
- DNS based blockades are good for global domain seizures but represent a very poor solution for content filtering purposes.
- Traffic redirection and encryption allow every enforcement to be circumnavigated, even with little effort.
- Internet security is compromised by most of the methods, with many potential side effects including human rights violation.

"Case of Yıldırım v. Turkey, Application no. 3111/10", European Court of Human Rights: http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-115705

- Feasibility is low for more effective methods (government cooperation needs and additional costs for hardware and software) and higher for less effective ones.

Conclusions

Efforts spent for years by ISPs and service providers to educate users about good practices and safe behaviors may be vanished by risky operations spread to bypass (improper) enforcements.

Moreover, the growth of new protocols developed to strengthen Internet security risks to be impaired or delayed.

Questions?