The worst part of censorship is XXXXX

Investigating large-scale Internet content

Sebastian Wolfgarten
http://www.devtarget.org

23C3, Berlin/Germany, December 29th, 2006

Outline

- Preface

1. Filtering techniques
   - Introduction
   - Network-level filtering
   - Application-level filtering
2. Filtering by example: China
   - Introduction
   - Practical implications
3. Circumventing the filtering
   - Overview
   - Defeating the “Great Firewall of China”

Hey, who the f*** are you?

- Just a random stranger interested in network security, penetration testing and IT forensics.
- Worked with Ernst & Young's penetration testing team in Germany and Ireland for four years.
- Currently part of T-Mobile's network security team in Germany.
- Formally graduated as Master of Science in Security and Forensic Computing.

<ad>Studying IT security</ad>

- If you are interested in getting a formal education in the area of IT security, consider a course offered by the Dublin City University (DCU) in Dublin/Ireland.
- The DCU is offering a one-year full-time Masters programme (called MSSF) which deals with IT security (e.g. the modules are including network security, secure coding, cryptography, formal software verification, biometrics, ...) as well as the practical investigation of computer crime and the principles underlying its prevention.
- Check out http://www.dcu.ie (-> Prospective students -> Postgraduate -> Faculty of Engineering & Computing) for more information.
- No, I am NOT paid to say this :-)

Motivation

- My Chinese room mate at DCU ("Censorship? What do you mean by that?").
- Curiosity.
- Consider recent events (blocking order in parts of Germany or allofmp3.com in Denmark).
- Large-scale Internet filtering is an area that still needs a lot of research.

Outline

- Preface

1. Filtering techniques
   - Introduction
   - Network-level filtering
   - Application-level filtering
2. Filtering by example: China
   - Introduction
   - Practical implications
3. Circumventing the filtering
   - Overview
   - Defeating the “Great Firewall of China”

Types of filtering

Network-level filtering

- Layer 3
- Layer 4

Application-level filtering

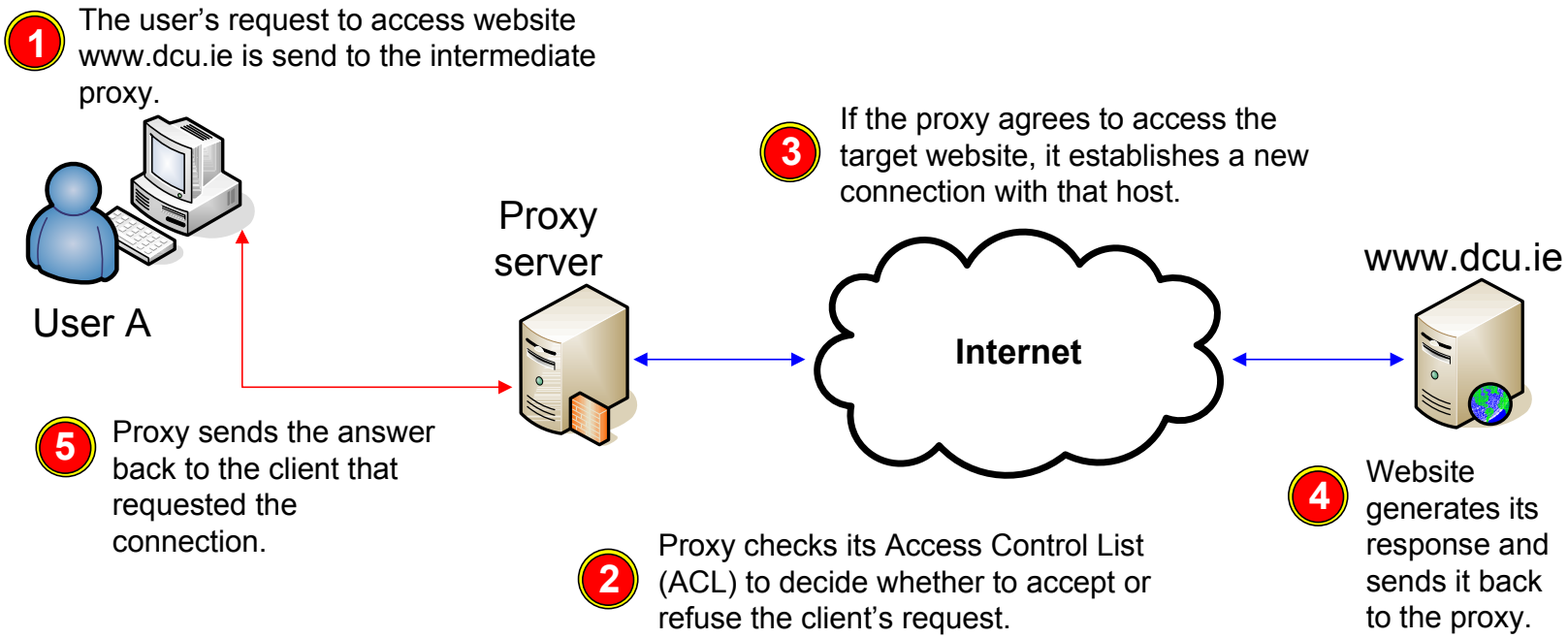
- Proxies
- Deep Packet Inspection
- DNS manipulations

Filtering & the OSI model

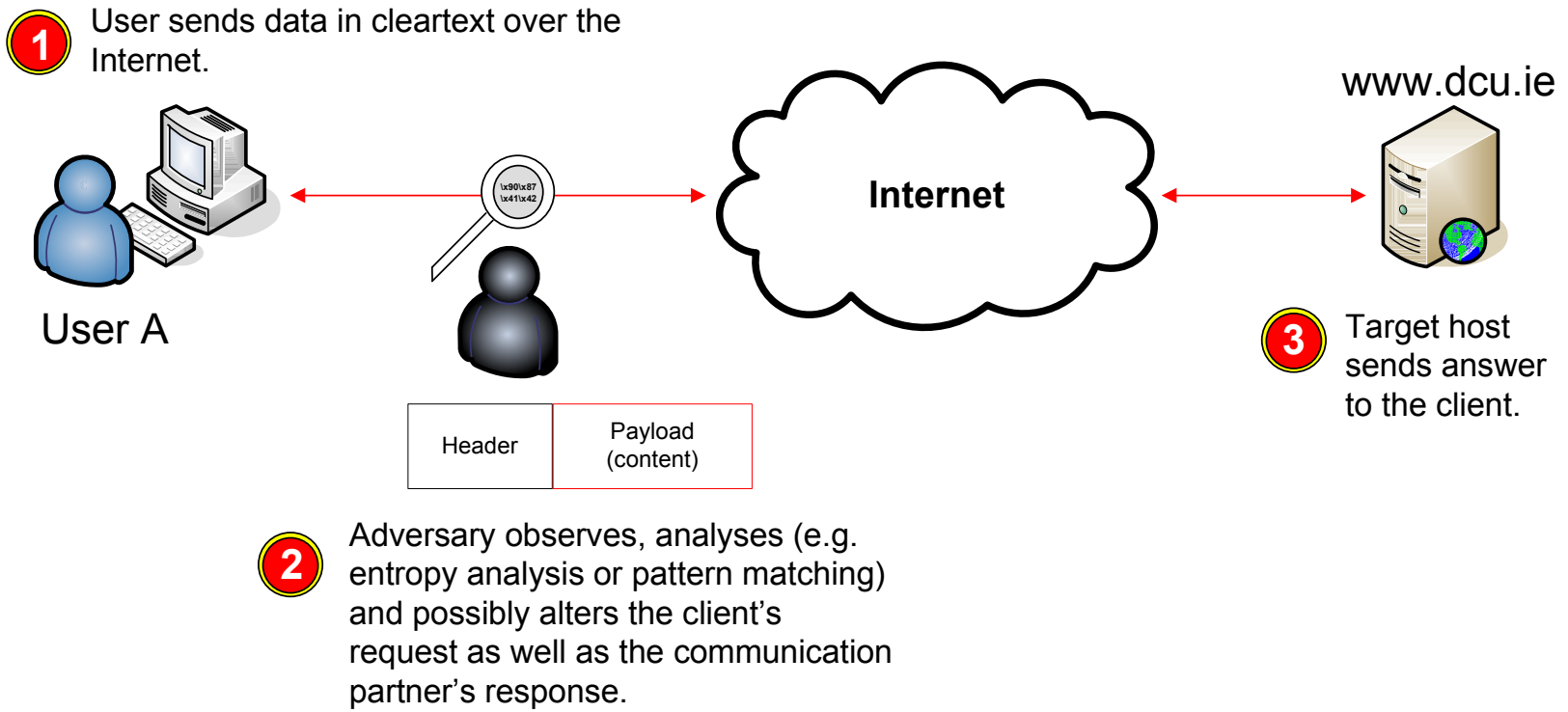
OSI model

#	Layer	Function	Example	Filtering mechanism
7	Application layer	Network process to application	HTTP, SMTP, SSH	Proxies, Deep Packet Inspection, DNS manipulations
6	Presentation layer	Data representation and encryption		
5	Session layer	Interhost communication		
4	Transport layer	End-to-end connections and reliability	TCP, UDP	deny tcp any host 213.133.109.150 eq 25
3	Network layer	Path determination and logical addressing	IP, ICMP	deny ip host 212.58.224.81 any deny ip any host 212.58.224.81
2	Data link layer	Physical addressing (MAC & LLC)		
1	Physical layer	Media, signal and binary transmission		

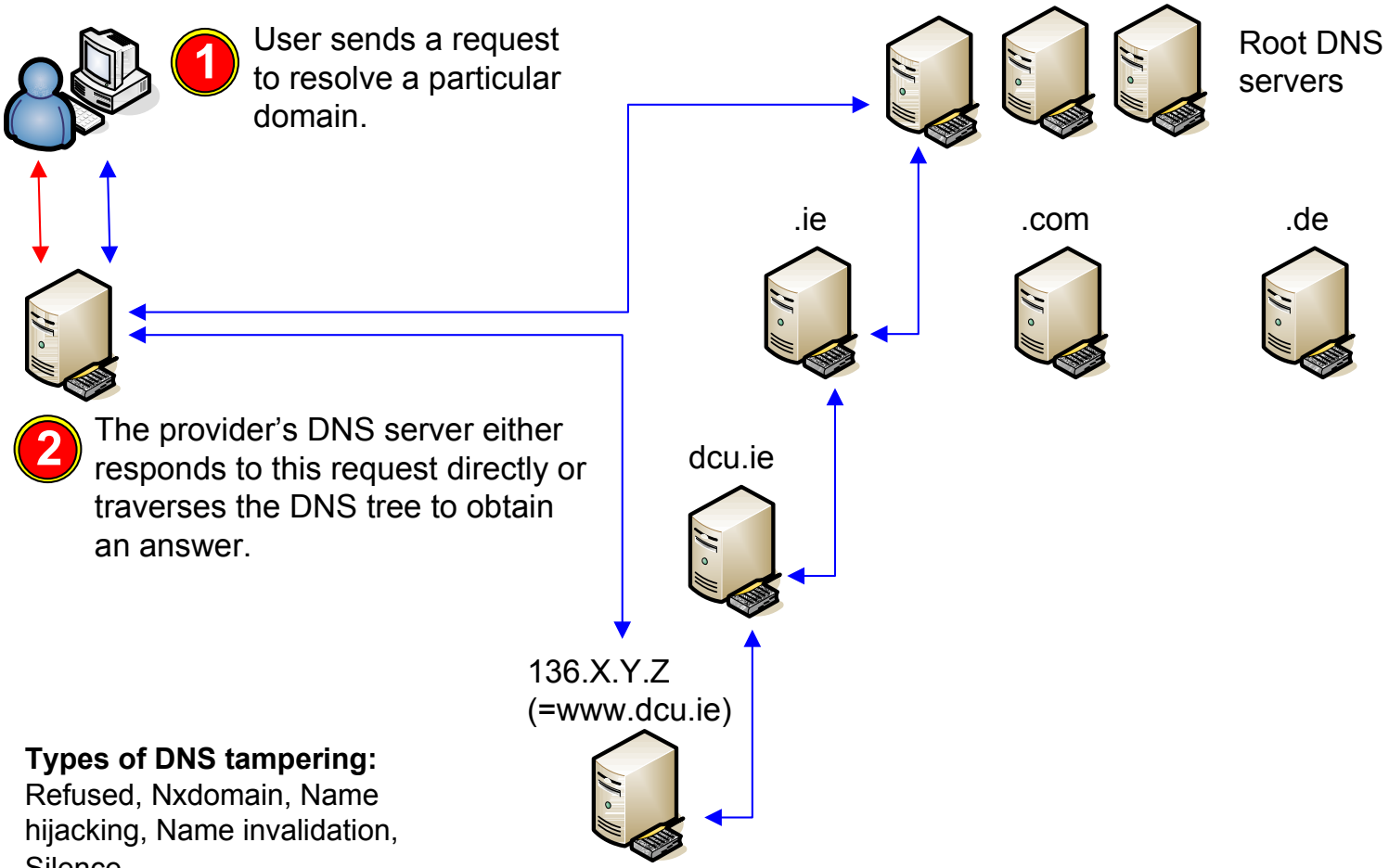
Proxy servers



Deep Packet Inspection



DNS manipulations



Types of DNS tampering:
Refused, Nxdomain, Name hijacking, Name invalidation, Silence

Demo #1 - DNS manipulations

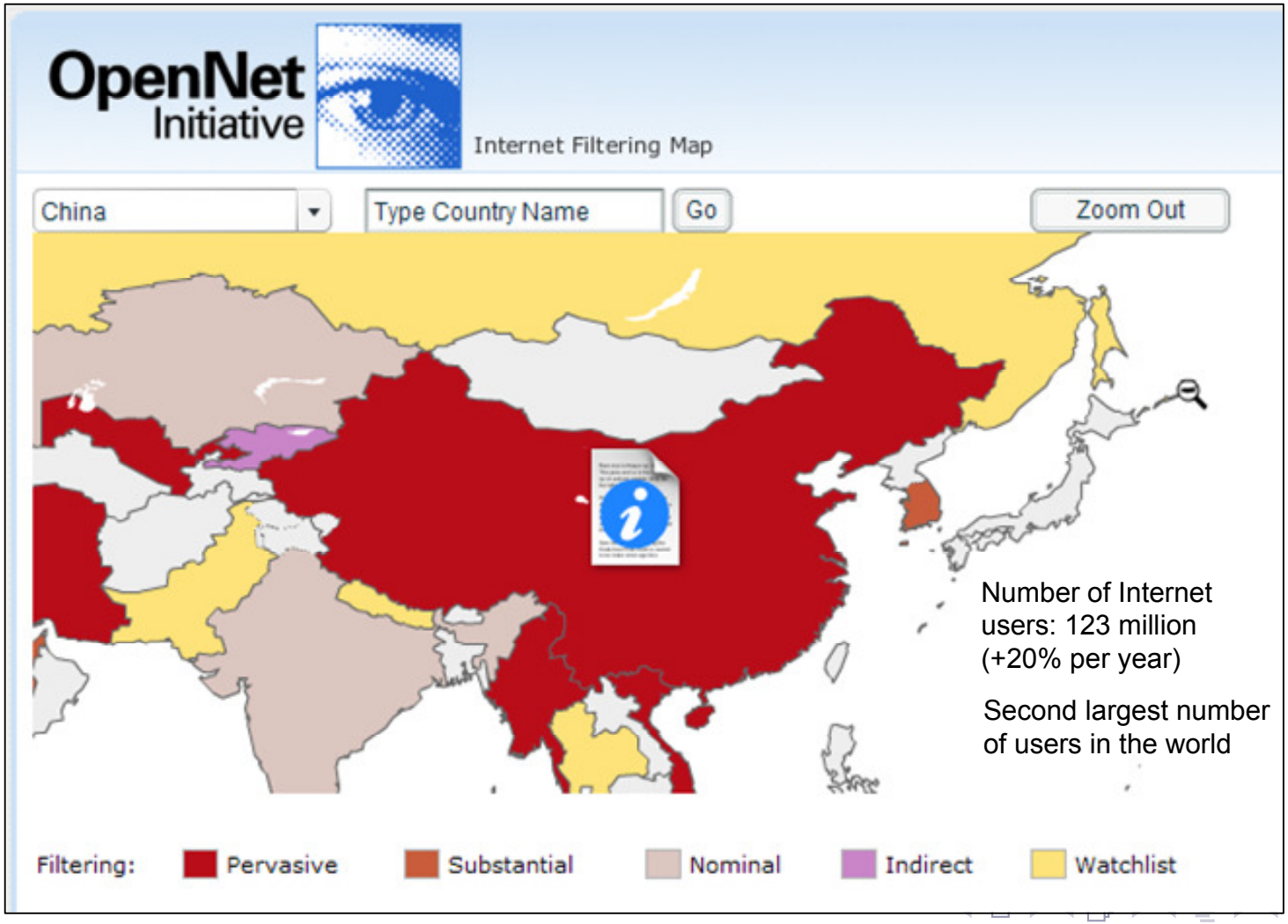
A demonstration of state-decreed DNS manipulations (“blocking order”) in North Rhine-Westphalia, Germany. These manipulations will prevent users based in this part of Germany from resolving and thus connecting to a number of Nazi-related websites (e.g. www.stormfront.org).

Outline

- Preface

1. Filtering techniques
   - Introduction
   - Network-level filtering
   - Application-level filtering
2. Filtering by example: China
   - Introduction
   - Practical implications
3. Circumventing the filtering
   - Overview
   - Defeating the “Great Firewall of China”

Introduction



Introduction (cont.)

Forbidden and thus blocked information are including (but not limited to):

- Any information contradicting the constitution of the Peoples Republic of China.
- Any information disclosing state secrets, violating national security, subverting the government or destroying the unity of the country.
- Any information damaging the honour and the interests of the state.
- Any information disturbing social order or undermining social stability.
- Any information spreading or instigating lewdness, pornography, gambling, violence, murder or terror.

The Domain Name System

- In order to discover whether this type of manipulation is used by the Chinese government, 50 sample domains were resolved simultaneously in an automated manner on a Chinese and a German server.
- The sample dataset contained the addresses of well-known political or religious organizations as well as television channels, newspapers and other popular domains.
- The German server resolved all 50 domains correctly, whereas the Chinese server failed to resolve approx. 20% of the samples.

The Domain Name System (cont.)

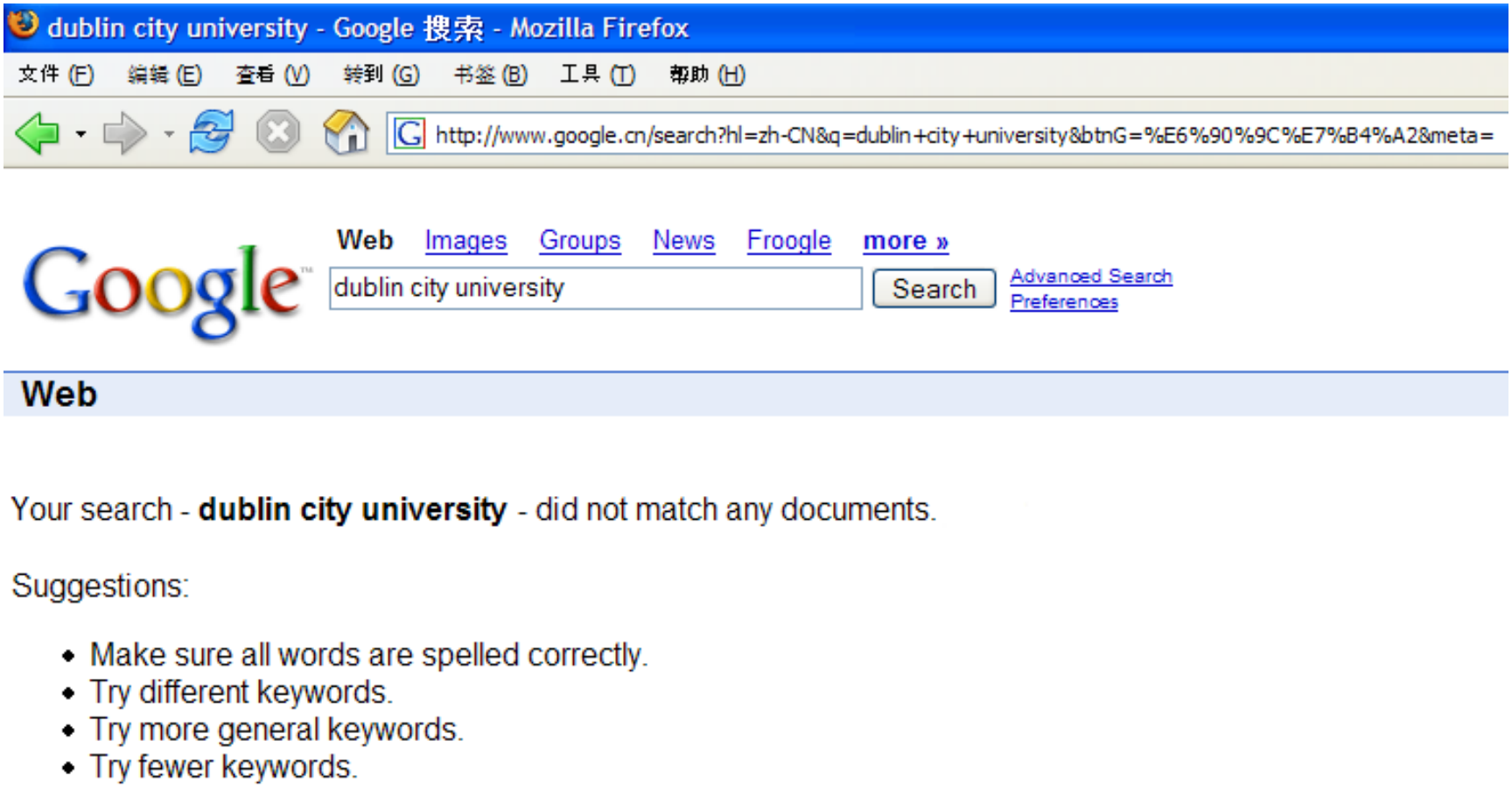
The following domains could not be correctly resolved in China:

Domain	Description	Result
www.falundafa.org	Spiritual movement	SERVFAIL
www.amnesty.org	Human rights org.	SERVFAIL
www.bbc.co.uk	Television channel	SERVFAIL
www.wikipedia.org	Online encyclopedia	SERVFAIL
www.cnn.com	Television channel	SERVFAIL
www.greenpeace.org	Non-profit organis.	SERVFAIL
www.playboy.com	Adult entertainment	SERVFAIL
www.gov.tw	Taiwanese governm.	Timeout
www.worldpress.org	News	Timeout

Demo #2 - DNS manipulations (in China)

The Chinese government employs DNS tampering to prevent users from resolving certain domains (e.g. www.amnesty.org).

Search engines

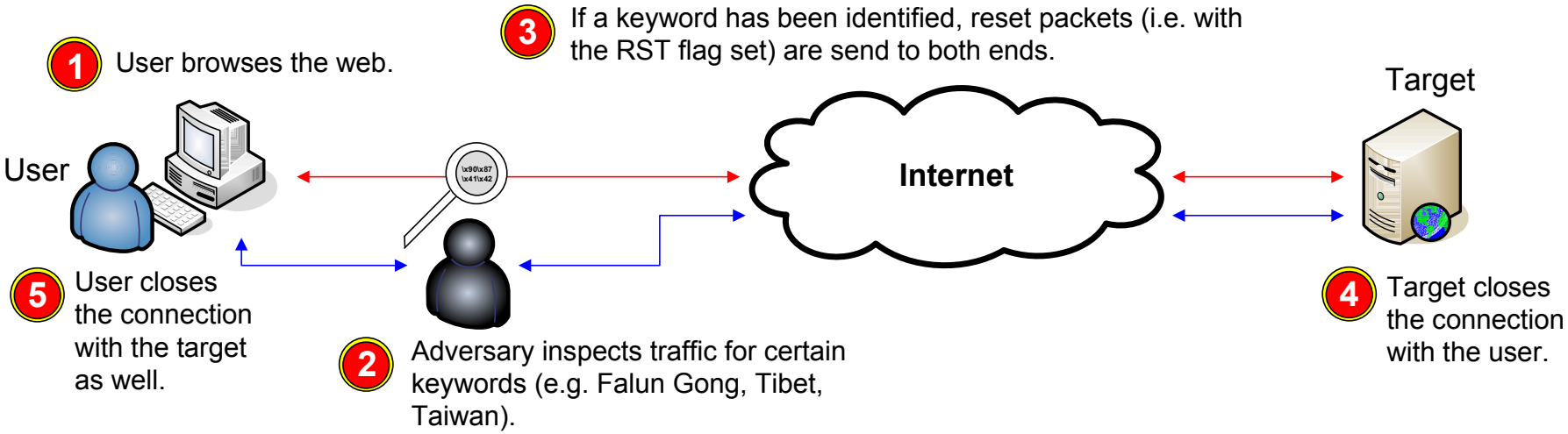


Search engines

All major search engines (e.g. MSN, Yahoo, Google, Baidu) are subject to filtering in China. The filtering is based on:

- Website de-listing: A manipulation in which an undesirable website is deliberately removed (delisted) from the list of search results.
- Keyword censorship: A technique that prevents users from searching for specific keywords.

Web browsing



Demo #3 - Forged RST packets

The traffic is inspected for certain keywords (e.g. Falun Gong, Tibet, Taiwan). Once such a keyword has been identified, the connection between the two communication partners is deliberately cut off by sending forged RST packets to both endpoints.

Outline

- Preface

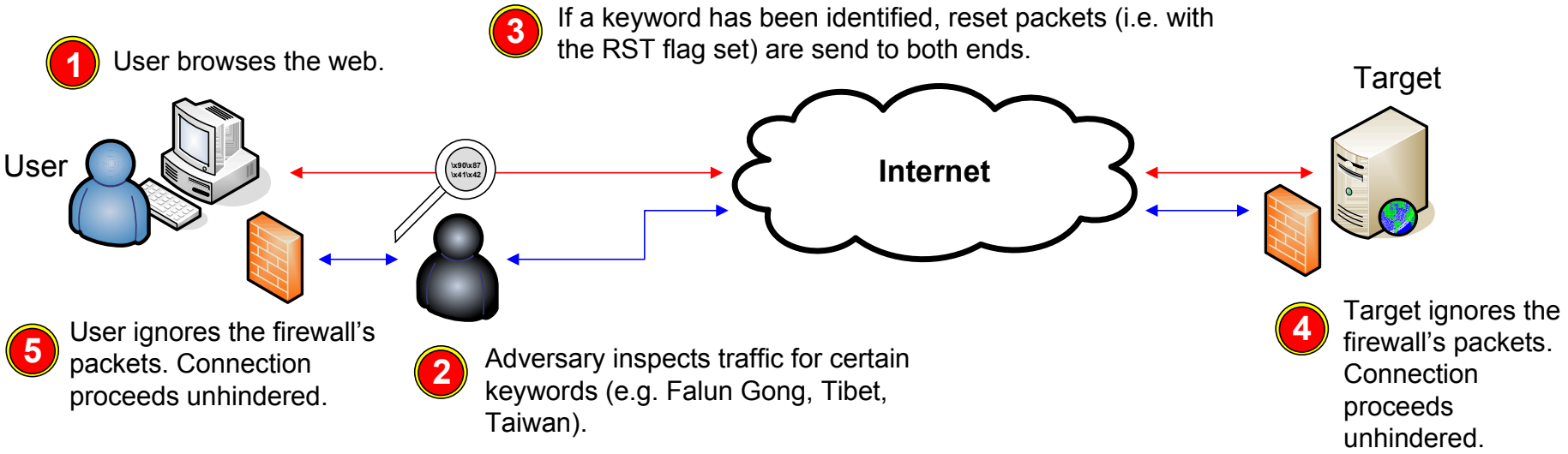
1. Filtering techniques
   - Introduction
   - Network-level filtering
   - Application-level filtering
2. Filtering by example: China
   - Introduction
   - Practical implications
3. Circumventing the filtering
   - Overview
   - Defeating the “Great Firewall of China”

Introduction

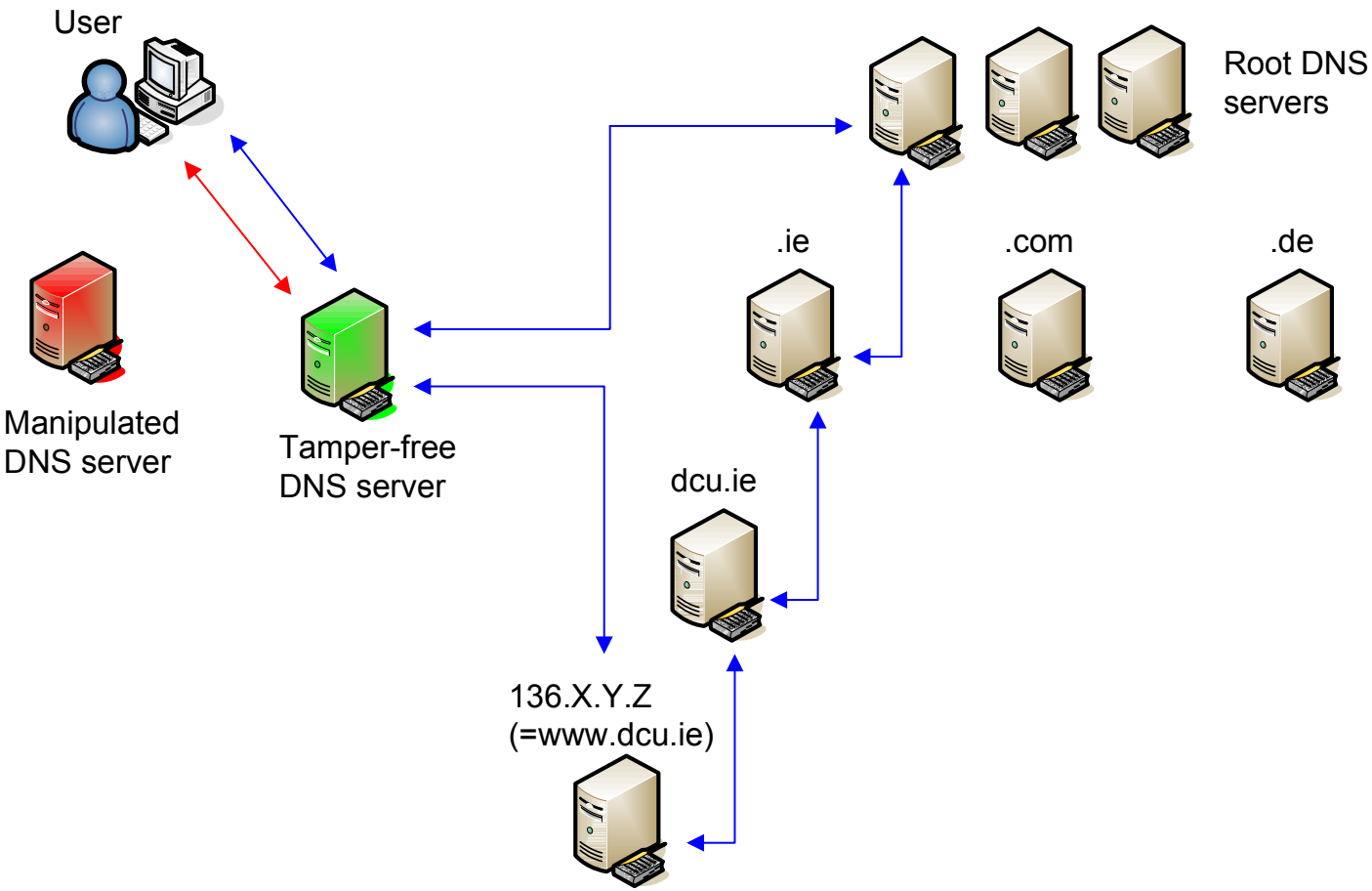
Given enough creativity and knowledge, every filtering can typically be circumvented in three steps:

1. Attempting to enumerate the magnitude and strictness of the filtering.
2. Making an educated guess about the functionality of the filtering mechanism (e.g. layer 3 or 4 filtering).
3. Selecting an appropriate circumvention technique based step 2.

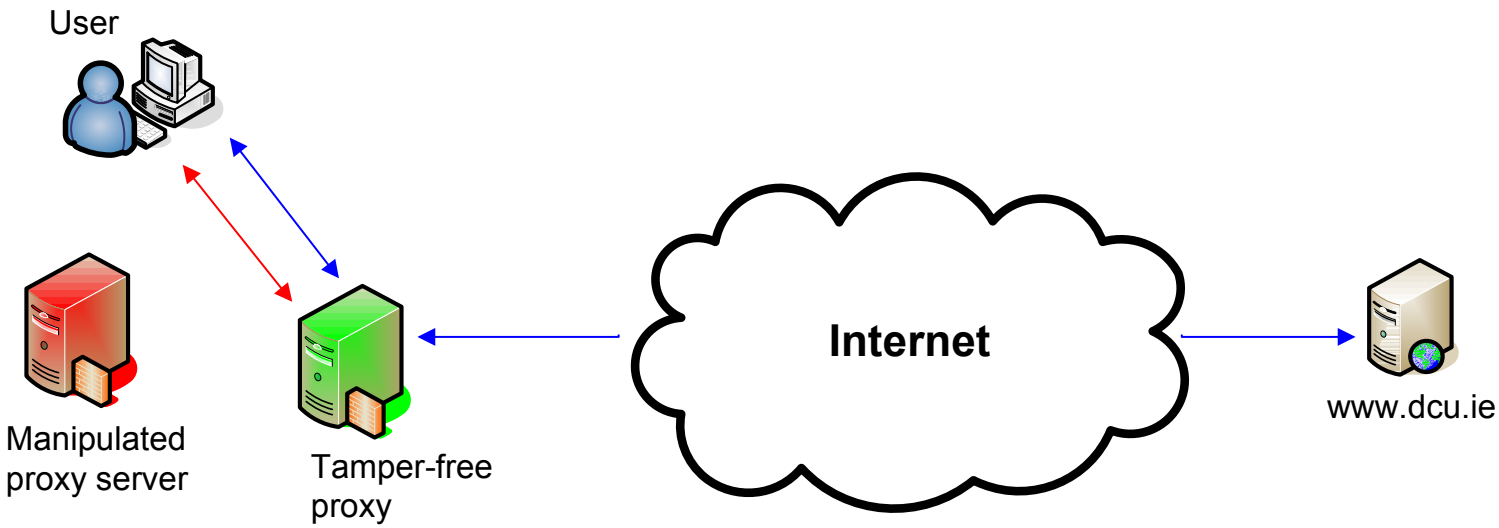
The Clayton method



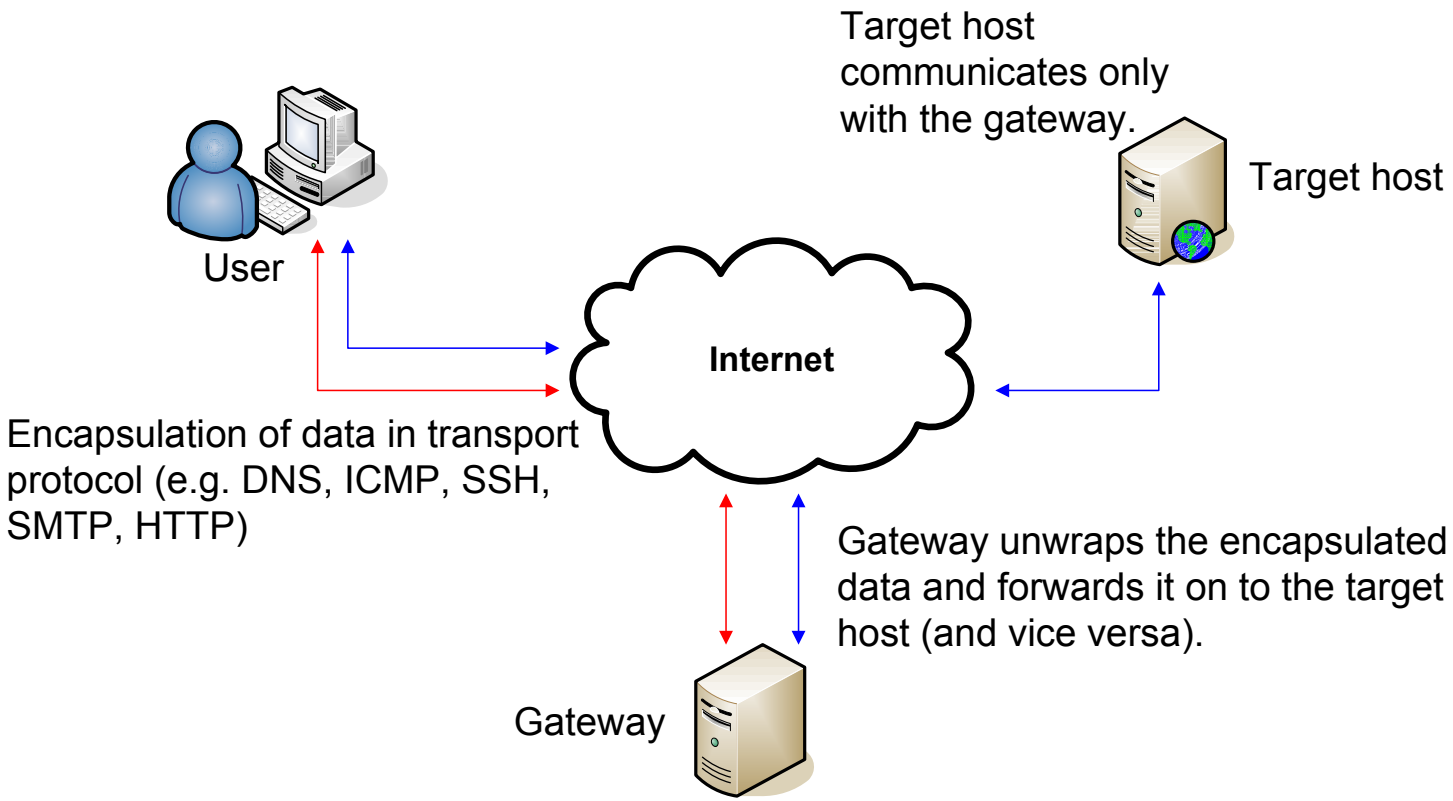
Alternative DNS servers



Alternative proxies



Tunneling


Target host
communicates only
with the gateway.
Target host
User
Internet
Encapsulation of data in transport
protocol (e.g. DNS, ICMP, SSH,
SMTP, HTTP)
Gateway unwraps the encapsulated
data and forwards it on to the target
host (and vice versa).
Gateway

Demo #4 - SSH tunneling

Probably the most elegant way of circumvention: Establishing a cryptographically secure tunnel to a remote system via SSH and forwarding a local port to a HTTP proxy server running on the same or even a different remote host.

Call for support

I am looking for people interested in doing some more research in the area of large-scale filtering. Gimme a shout if you are interested.

Summary

- The Chinese government operates the most extensive and pervasive system of Internet filtering in the world.
- This practicum investigated a variety of techniques to successfully circumvent this filtering.
- However in order to enable even the average user to defeat the filtering, other and especially easier circumvention methods must be developed...

That's it, folks.

Thanks for listening. I am now looking forward to answering your questions.