Network Traffic Monitoring and Tunneling for Censorship

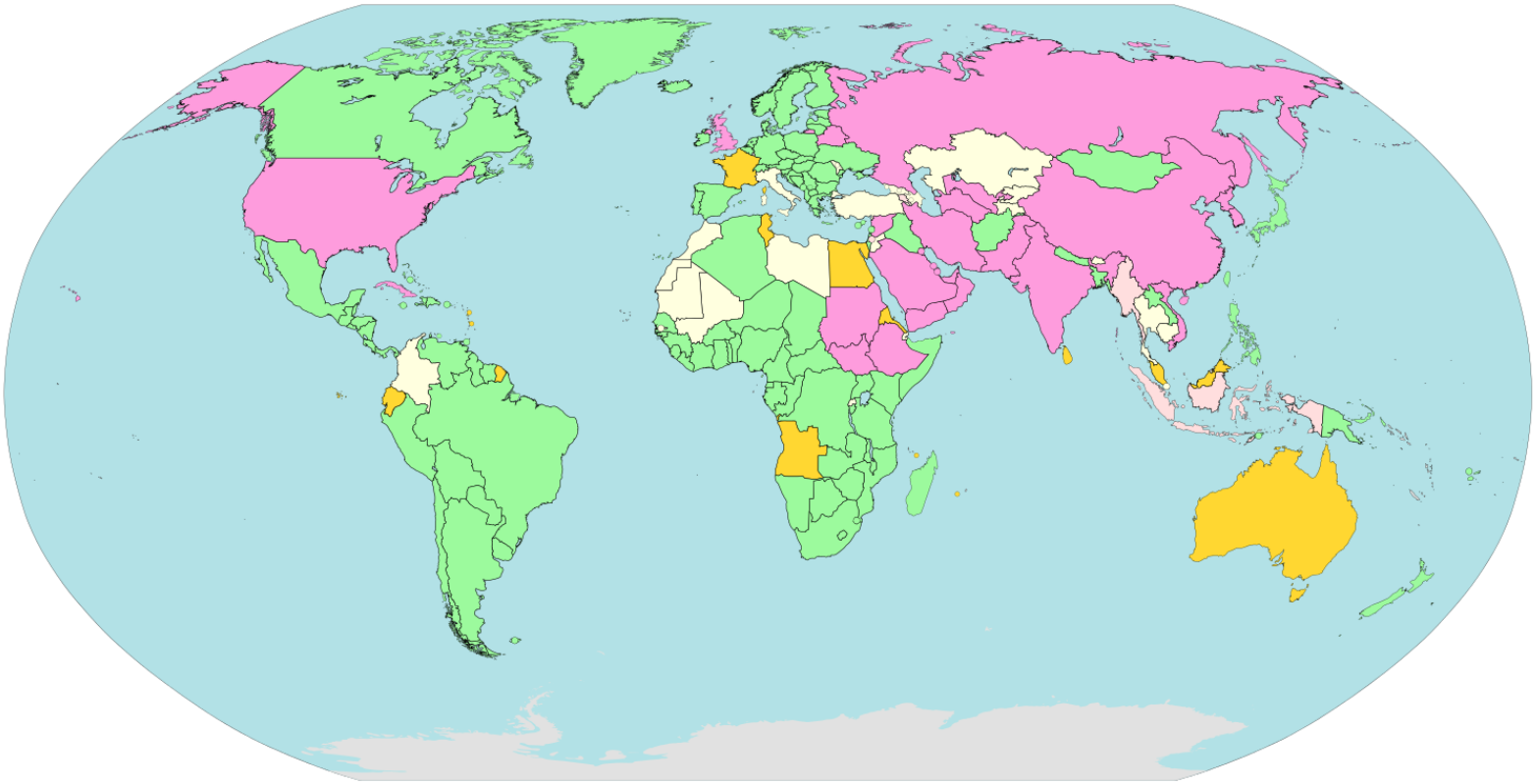
barkın kılıç

internet ungovernance forum 2014

about me: barkın kılıç

information security expert
head of dragon labs at
Comodo Ankara
tw: @BarknKilic
email: barkin@barkin.info

internet censorship ratings



[*OpenNet Initiative*, 2012]
[*Internet Enemies*, 2014]

surveillance in Turkey is widespread...

"Google received requests from the Information Technologies Institute (BTK) to remove 426 YouTube videos, some that criticized 'Ataturk, the government, or national identity and values'"

– *Google Transparency Report*

"Google BTK tarafından Youtube'un 'Atatürk'ü, devleti, ya da ulusal kimlik ve değerleri' eleştiren 426 videoyu kaldırmasını istedi"

– *Google Transparency Report*

TURKEY

29 women and men in the city of Izmir, Turkey, are being prosecuted for sending tweets during last year's protests across the country. All 29 people are being accused of "inciting the public to break the law" and could face up to three years in prison.

ETHIOPIA

On 17 July 2014, seven members of the Zone 9 blogging collective and three independent journalists were formally charged with terrorism offences and "Outrages against the Constitution" in Ethiopia. Ethiopia regularly uses the flawed Anti-Terrorism Proclamation to silence dissenting voices.

SAUDI ARABIA

In mid-2013, the authorities attempted to ensure that all encrypted social networking applications such as Skype, WhatsApp, Viber, and Line are fully monitored or outright banned. Raif Badawi...was arrested on 17 June 2012 and initially charged with "apostasy", a serious crime that carries the death penalty in Saudi Arabia. He was first sentenced to seven years in prison and 600 lashes for violating Saudi Arabia's IT law and insulting religious authorities through his online writings.

USA

NSA subcontractor Edward Snowden left his home in Hawaii for Hong Kong carrying intelligence documents that revealed the existence of vast surveillance programs led by the USA's National Security Agency (NSA) and the UK's General Communications Headquarters (GCHQ).

twitter

"Şu anda Twitter denilen bir bela var...Sosyal medya denilen şey aslında şu anda toplumların baş belasıdır"

- Erdoğan

"There's a nuisance right now called Twitter... What we call social media is actually the common worry of societies"

- Erdoğan

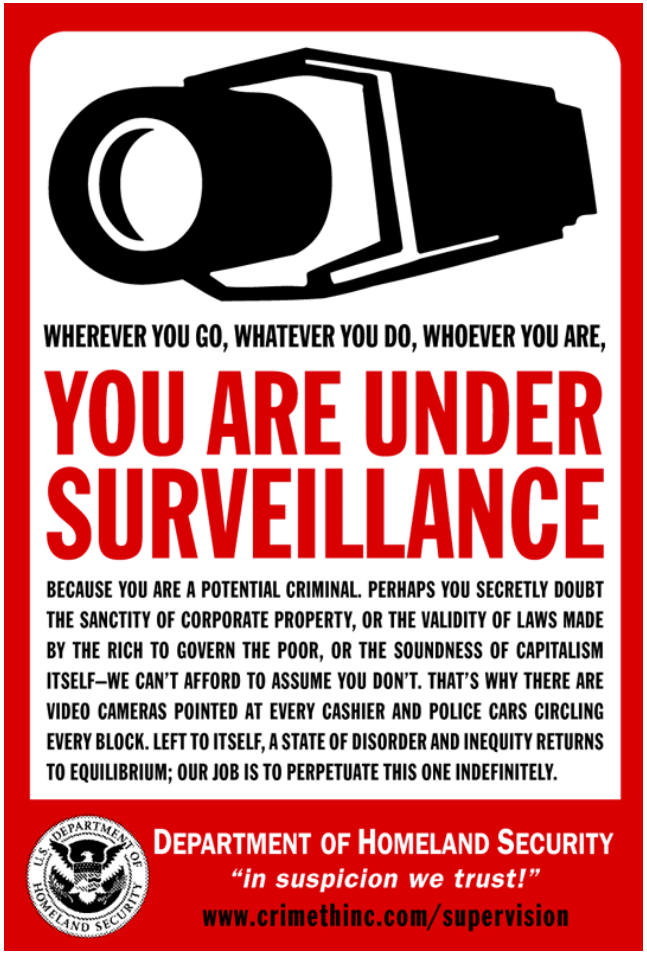
WHO Has Your Back?

Which companies help protect your data from the government?

	Requires a warrant for content	Tells users about government data requests	Publishes transparency reports	Publishes law enforcement guidelines	Fights for users' privacy rights in courts	Fights for users' privacy rights in Congress
amazon	☆	☆	☆	☆	★	★
Apple	☆	☆	☆	☆	☆	★
at&t	☆	☆	☆	☆	☆	★
comcast	☆	☆	☆	★	★	☆
Dropbox	★	★	★	★	☆	★
facebook	★	☆	☆	★	☆	★
foursquare	★	★	☆	★	☆	★
Google	★	☆	★	★	★	★
LinkedIn	★	★	★	★	☆	★

commonly used methods for censoring internet content

> IP blocking
> Domain Name System filtering & redirection
> URL filtering
> Deep Packet filtering
> Connection reset
> Web feed blocking
> Reverse surveillance
> Self censorship

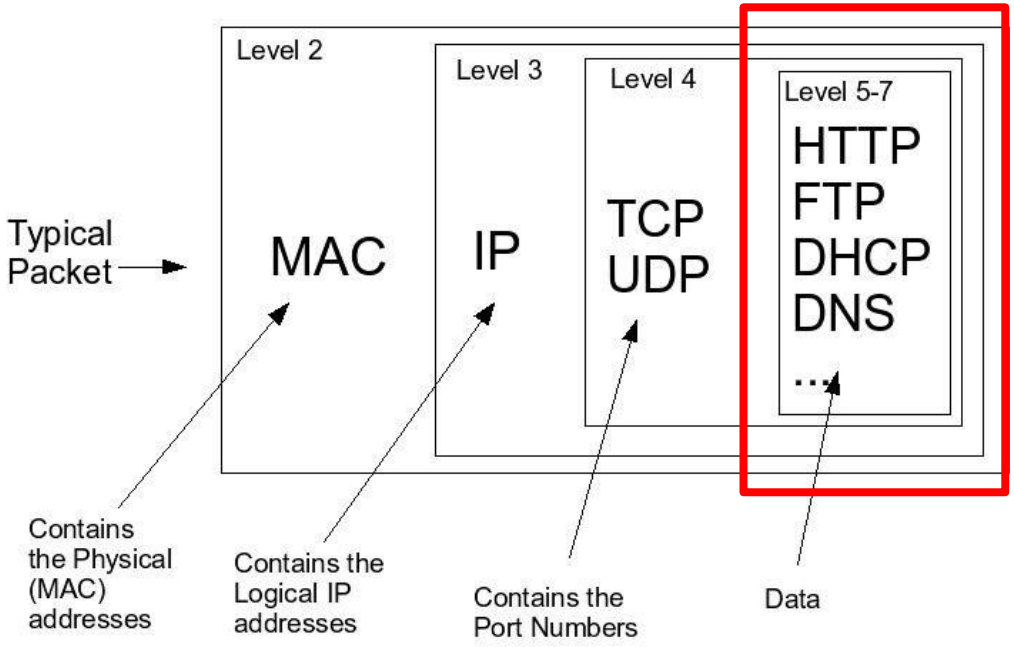


what is a network packet?

> a network packet is one unit of binary data capable of being routed through a computer network

> they are formed by at least 20 bytes of headers

> data is transferred over networks by chunks of network packets



* this is the part they are after!

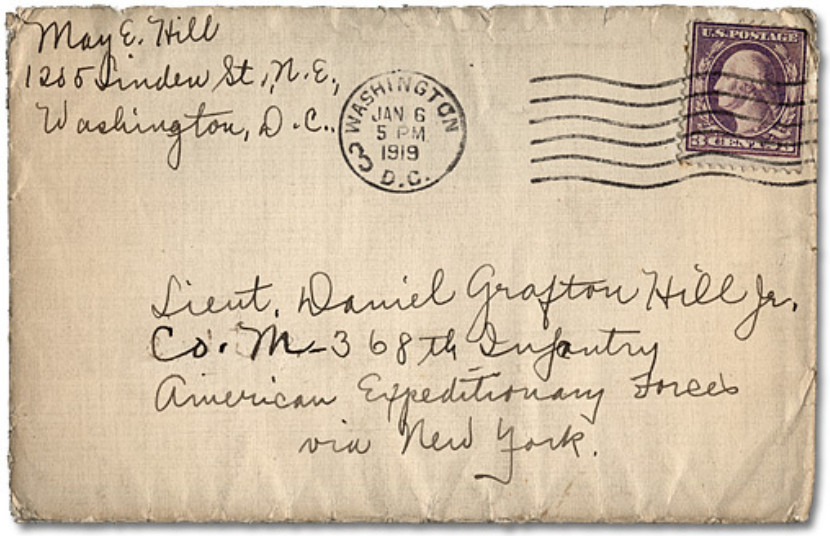
Packet - E-mail Example

Header	Sender's IP address Receiver's IP address Protocol Packet number	96 bits
Payload	Data	896 bits
Trailer	Data to show end of packet Error correction	32 bits

header

> the envelope, has the header information

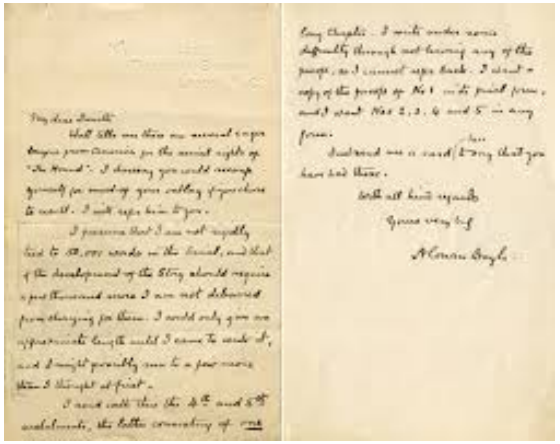
> determines where the package goes



payload

> the letter, with the real data (and what you want to get to)

> the data that you want delivered



deep packet inspection

> the header and payload are processed and examined to discover what content it's containing

> ex: blocking a Twitter account

methods for sniffing packets

> for local networks and wifi, MITM (man in the middle) methods

> using/changing routing protocols for re-routing

> poison DNS caching/take it over

> physically mirroring a port to another one with your cable

data carving

> obtaining original data from a binary document (.pcap or other format) created by using Sniffer

> monitors flowing network traffic

> these methods can listen, see, and save anything that is done between two points of contact

> basis of Network Forensics

bypassing internet censorship: counter methods

> Proxy websites

> Java Anon Proxy

> Virtual Private Networks (VPN's)

> Tor

encryption placement and application

> encryption: two parties communicating only with each other, securely

> can tell that a conversation is going on from the outside, but can't decipher what is being said

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.12 (GNU/Linux)

9898cBAEBAgAGBQJT9iRTAAoJEBLZTB73Wt+tN8UIAKZW1vYbZPjLFupQb/sJh7EGeVvbE+WoNFoAXq8dZAeujZJSyIZ1dNDGmDHxX12bY
vwEAFJxovR998mM8Z7wNrL+RopqrBikBOATCVd7nCtTdUdrhoblIqhwOhqVn+wR/nTBaYqHEp3fXDQ41mbSoUTwq

pVx56uDRDEq75WfAzCNuXI/rfOLOI6kzlXOvsQjcEuT/PX/1FfscUWz8sYwoVher+W1CJTe7zmlIxeggDyceGRCQzlA6erQmrEiIc8B1NzU
1nUuuC798YafIaFqJtu42YIyRsNYk0oeXycdWqmwGqjIxemoqhhO2SySeXzEddwLJBuWp2fmueeOFvWNWqdBp0=

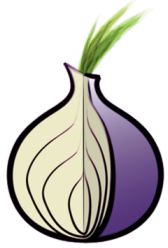
=A31N

-----END PGP SIGNATURE---

internet monitoring & censorship

pros	cons
> protect those who can't protect themselves (minors, etc) > private companies may use it to increase productivity > ?	> ethically/morally wrong > hinders social connections and access of resources > encourage people to illegally access points of information

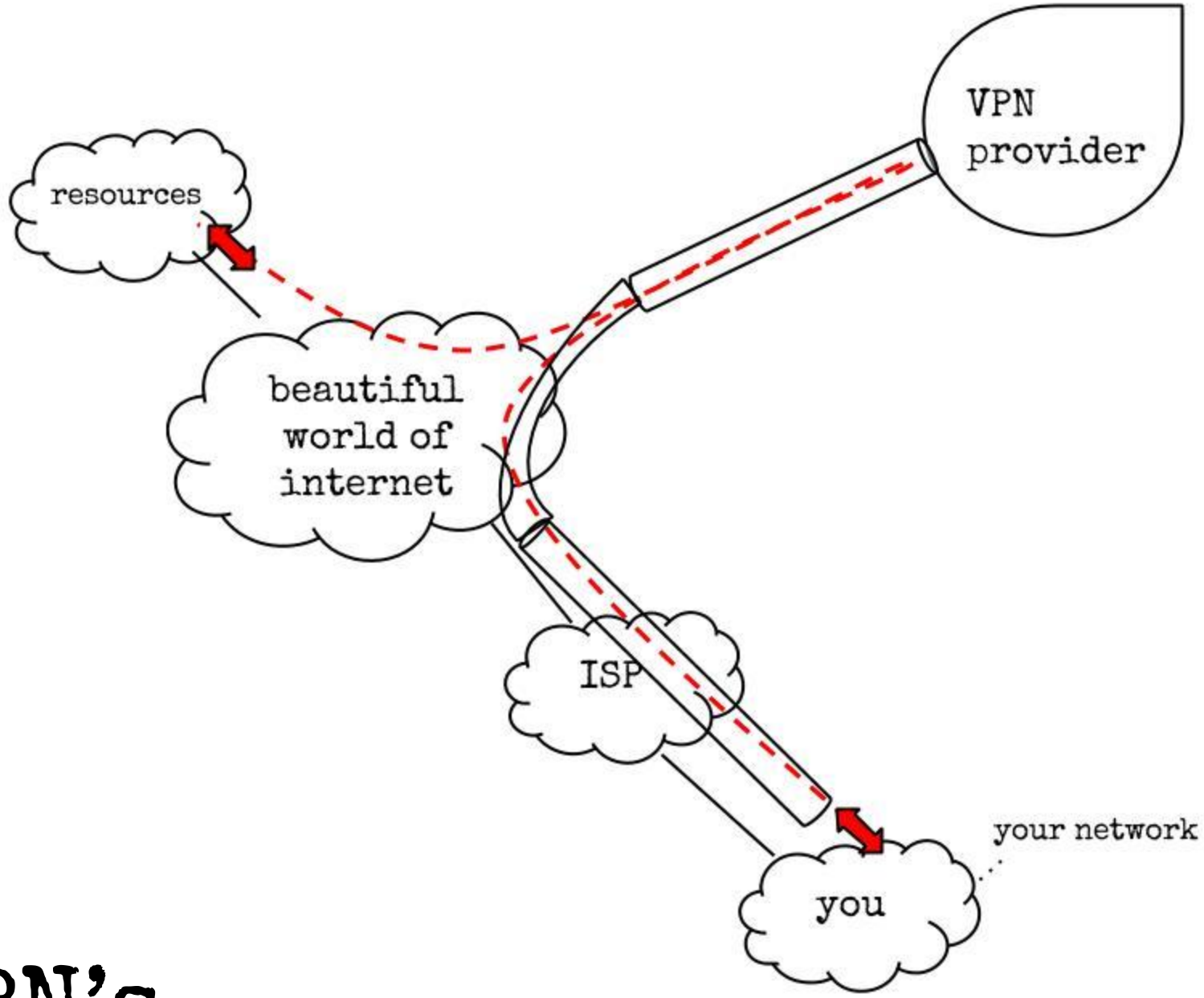
case study: tor



> prevents people from learning your location or browsing habits

> a network of **virtual tunnels** that allows people and groups to improve their privacy and security on the Internet

> people who use Tor: journalists, NGOs, whistleblowers, anyone who wants to


VPN
provider
resources
beautiful
world of
internet
ISP
your network
you

VPN's

important

If you care about access but not privacy:

> VPNs (instead of trusting your ISP, you are trusting your VPN provider)

> Tor is just the same (you are anonymous but your data can still be seen)

The only way to be private online:

> SSL or

> point-to-point encryption

What is SSL?

> Secure Sockets Layer (SSL)/TLS

> a sub-layer protocol developed to give encryption to insecure protocols

> HTTPS= TLS + HTTP or SSL + HTTP

> only provides data protection during communication, does not protect against security breaches of the target system

certificate authorities

> has the job of authenticating a SSL concept and making sure it becomes widespread

> a certificate authority holds all the power of SSL security

> a security issue with a certificate authority can affect all SSL users, not just the ones using the authority

monitoring encrypted traffic

> need several conditions to intercept a SSL connection:

1- must be routed to pass from the target system's traffic

2- must create a fake certificate with the information given by the HTTPS page the system is trying to connect with

> this fake certificate will give the user a warning, but how severe depends on the browser

beating SSL

> a certificate authority is useless on its own, it must be recognized as legit by the client's side

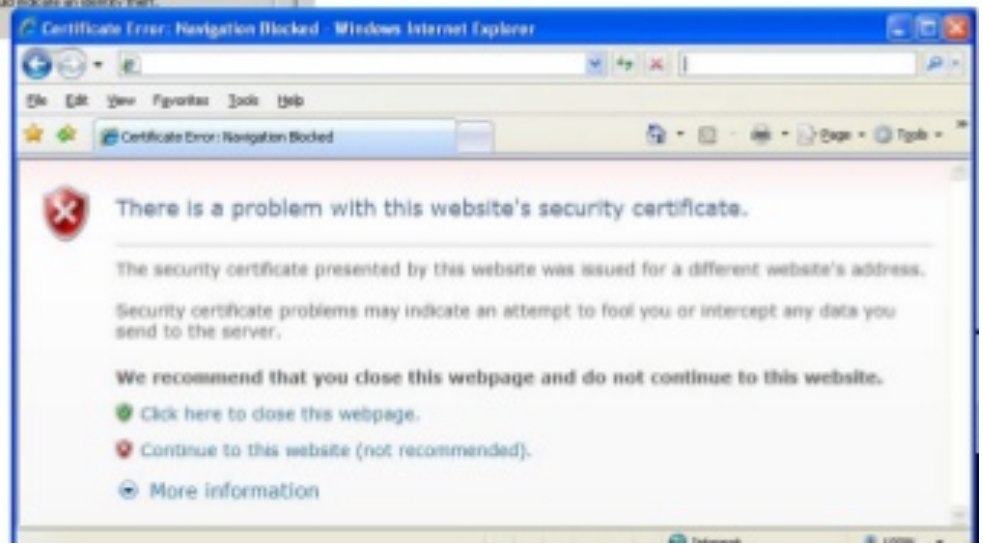
> hacking one worldwide SSL authority and obtaining the secret key used in certificate production might make SSL usage pointless!

> certificates approved by a trusted certificate authority will function normally

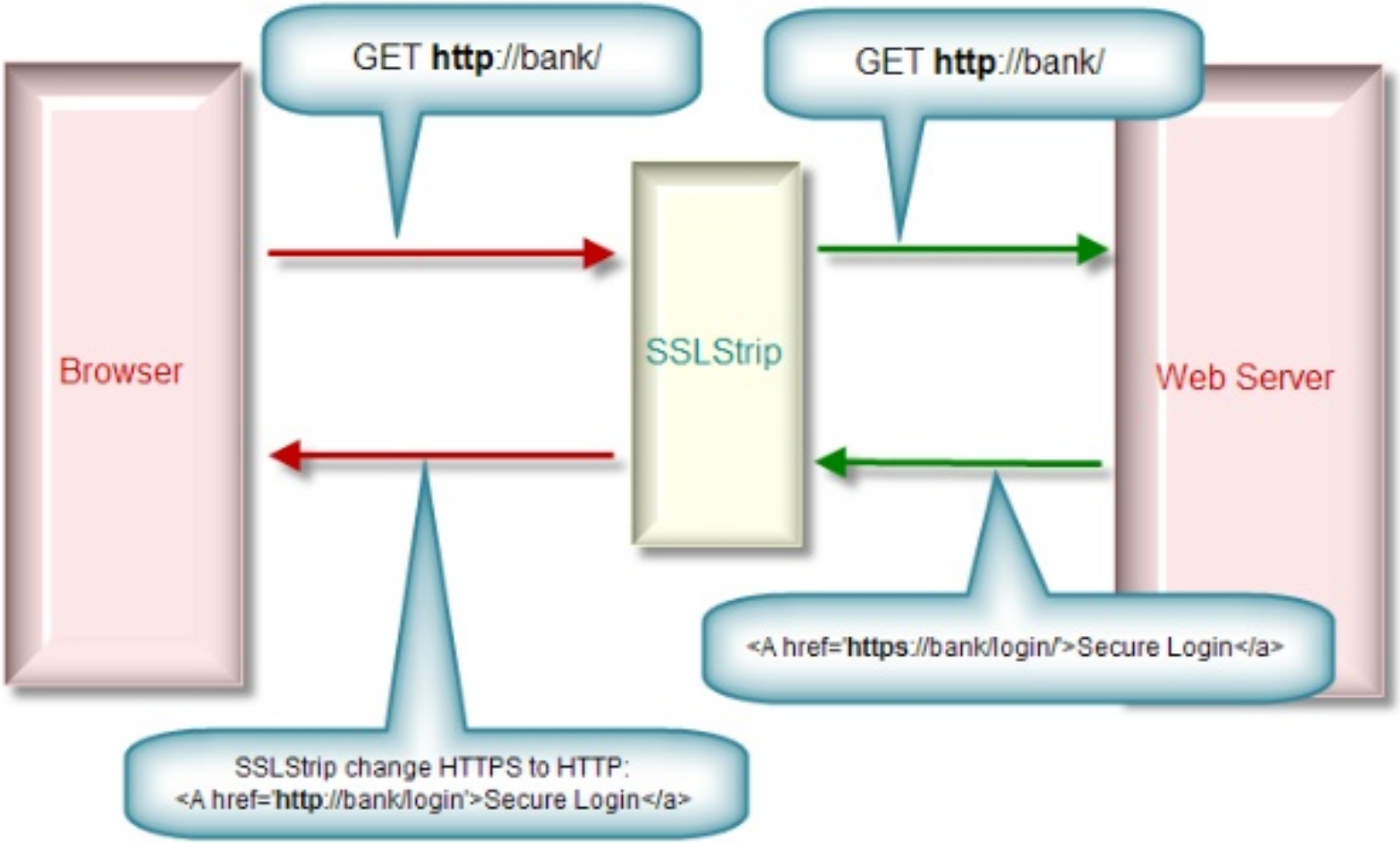
OLD Method - SSL MITM

Firefox

Internet Explorer 7



New Method - SSL Strip



More Modern Way - Inject Trusted Certificate

thank you!
teşekkürler!

github.com/averagewizard for slides
and list of resources