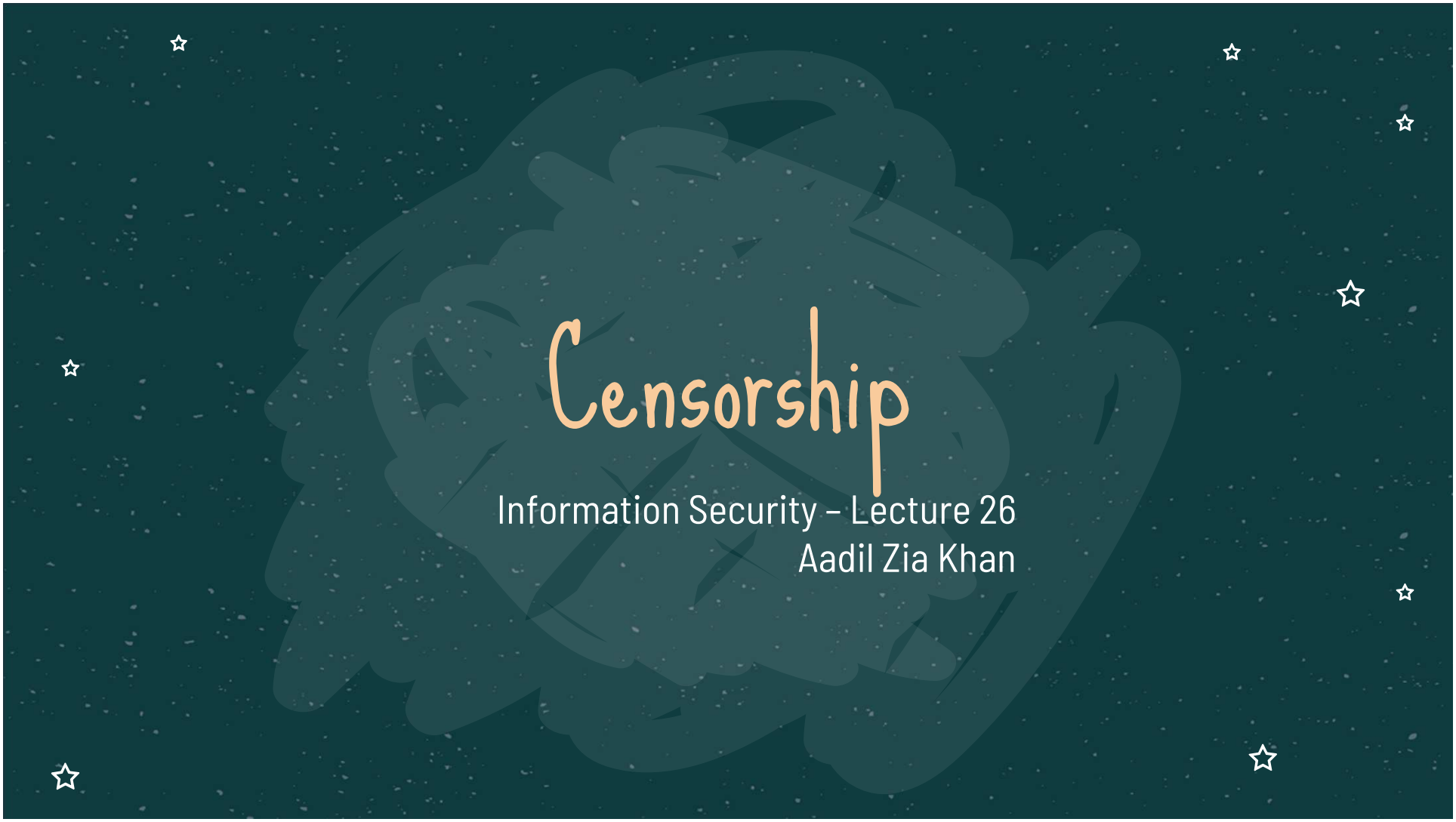

Censorship
Information Security – Lecture 26
Aadil Zia Khan


GREAT FIREWALL OF CHINA
Google
YouTube
facebook.
Gmail

Censorship

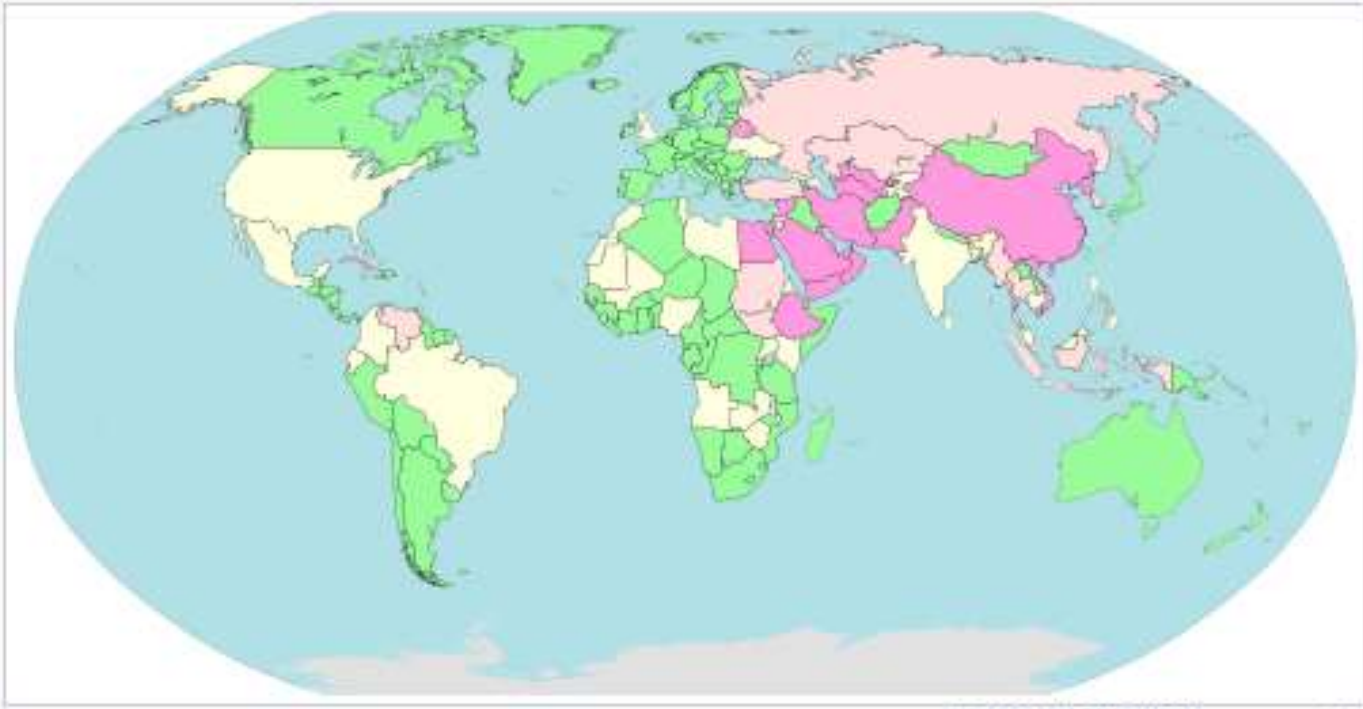
Internet censorship is the control or suppression of what can be accessed, published, or viewed on the Internet enacted by governments and private regulators

Why Governmental Censorship

- Governments ban websites and application because of:
  - Political philosophy
  - Religious beliefs
  - Social norms
  - Security concerns
  - Protection of existing economic interests and copyright
  - Right to be forgotten

Governmental Censorship Examples

- Pakistan had banned youtube, imdb because of blasphemous content
- There was a time we couldn't access Israeli university pages from Pakistan
- Muslim countries usually ban obscene content
- Copyrighted, and pirated material like piratebay and sci-hub is usually blocked
- Content targeting an individual can be blocked and removed – as was done by Beyonce
- Terrorist websites can be blocked for security purposes
- Communication links can be blocked during protests
- China has banned … it would be easier to list what they have not banned ☺



Internet censorship and surveillance by country (2018)[83][84][85][86][87]

- Pervasive: *Large and broad*
- Substantial: *Medium*
- Selective: *Small and specific*
- Little or no
- Not classified / no data

Private Censorship

- Many organizations ban apps and websites (or transport protocols used for these) that would impact productivity
  - Social Media (Facebook, Twitter, Insta)
  - Video Sites (Youtube)
  - UDP (because company related traffic is usually TCP)

Censorship - Control Points

Taken from wiki

- Internet backbone, Internet exchange points (IXP), operators of submarine communications cables, satellite Internet access points, international optical fibre links etc.
- Internet Service Providers, install voluntary (as in UK) or mandatory (as in Russia) Internet surveillance and blocking equipment
- Individual institutions, implement some form of Internet access controls to enforce their own policies, or may be forced to do this by the government
- Personal devices, whose manufacturers or vendors may be required by law to install censorship software

Censorship - Control Points

- Application service providers (e.g. social media companies), may be legally required to remove particular content
  - E.g. governments ask Twitter to remove tweets (with threat of complete closure and subsequent financial loss)
  - E.g. USA prevents its companies from dealing with Iran
- Certificate authorities may be required to issue counterfeit X.509 certificates controlled by the government, allowing man-in-the-middle surveillance of TLS encrypted connections
- Content Delivery Network providers who tend to serve large amounts of content (e.g. images) may be an attractive target for censorship authorities

Censorship - Approaches

Taken from wiki

- Internet Protocol (IP) address blocking
  - Access to a certain IP address is denied
  - If the target Web site is hosted in a shared hosting server, all websites on the same server will be blocked
- Domain name system (DNS) filtering and redirection
  - Blocked domain names are not resolved, or an incorrect IP address is returned
  - External DNS may be blocked so that users may not use them as alternative DNS

Censorship - Approaches

- Uniform Resource Locator (URL) filtering
  - URL strings are scanned for target keywords regardless of the domain name specified in the URL – dropping the HTTP request packets that include forbidden keywords
- Packet filtering
  - Terminate TCP packet transmissions when a certain number of controversial keywords are detected
- Network disconnection
  - Simply cut off all routers completely; either by software or by hardware (turning off machines, pulling out cables)

Censorship - Approaches

- Portal censorship and search result removal
  - Portals and search engines, may exclude web sites that they would ordinarily include - rendering a site invisible to people who do not know where to find it
    - E.g. Google.de and Google.fr remove Neo-Nazi and other listings in compliance with German and French law

- Computer network attacks
  - Denial-of-service attacks and attacks that deface websites can prevent or limit access to certain websites or other online services

Censorship - Circumvention

- Proxies and ToR browser - if some address/protocol/keyword is blocked, we can route our request through a proxy or using ToR
  - Request would be forwarded (and returned) through an intermediary node, the packet's source address would be of that node and not the original server's blocked address
  - If some protocol is blocked, proxies can wrap the packet inside their own packet header in order to hide the original protocol
  - If some keyword is blocked, the proxies can encrypt the data

Censorship - Circumvention

- Alternative DNS
  - In case the DNS does not resolve the address because of censorship, a DNS in another country can be used
  - e.g. 8.8.8.8
- Bypass DNS if the IP address is known (and is not itself blocked)
  - Type the IP address instead of the domain name as part of a URL given to a Web browser

Censorship - Circumvention

- Encrypted protocols
  - E.g. TLS/SSL and HTTPS
  - Since they encrypt the packets, and blocks due to keywords or URLs will be circumvented
  - Note when using the basic HTTPS, the domain name is left unencrypted in the handshake – some extensions fix that
- Satellite ISP to access Internet
  - If the telephone and Internet services are blocked, the only option left is to use satellite services
  - Note that since these are wireless, they can be jammed

Proxies & Advertising

- Internet advertising is based on
  - User behavior (identified through cookies)
  - Geolocation (identified through IP address)

- When a request is forwarded through a proxies, the source address that the server sees is of the proxy (and not the original user)
  - Geolocation based services (including advertising) fail because of this

slidesgo