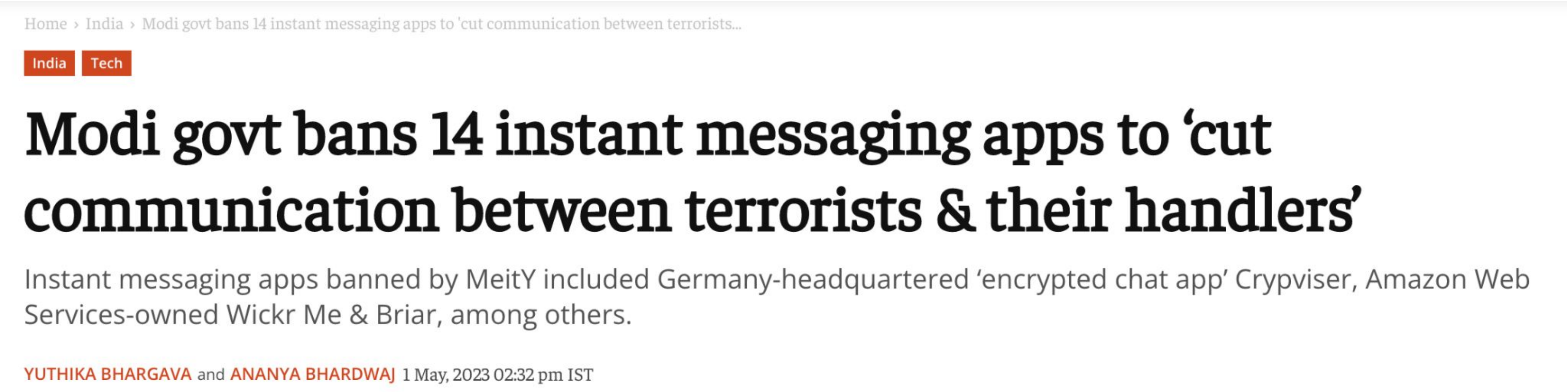
CS558 Network Security

Lecture n: Review



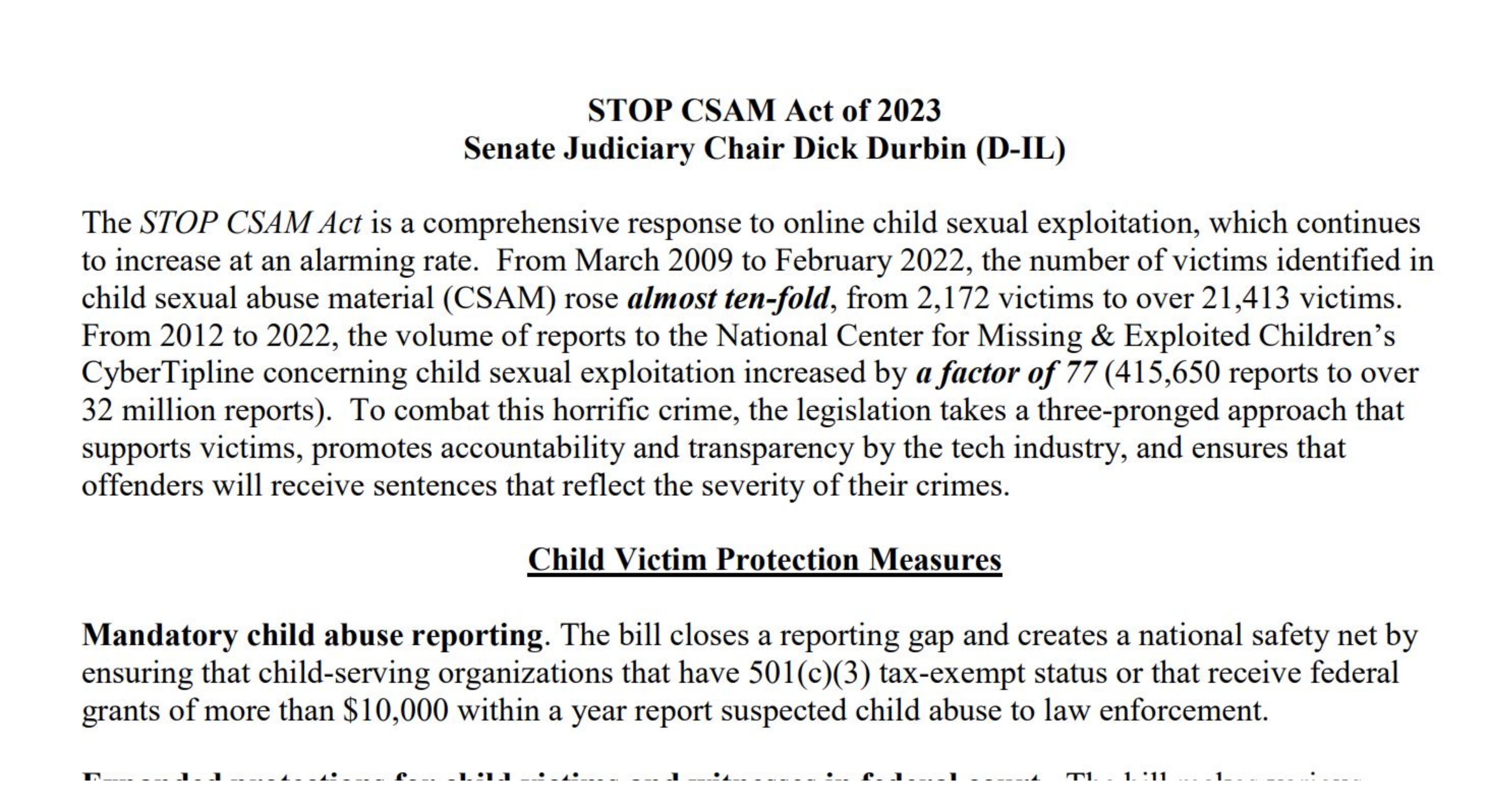
Home › India › Modi govt bans 14 instant messaging apps to 'cut communication between terrorists...

India Tech

Modi govt bans 14 instant messaging apps to 'cut communication between terrorists & their handlers'

Instant messaging apps banned by MeitY included Germany-headquartered 'encrypted chat app' Crypviser, Amazon Web Services-owned Wickr Me & Briar, among others.

YUTHIKA BHARGAVA and ANANYA BHARDWAJ 1 May, 2023 02:32 pm IST



STOP CSAM Act of 2023
Senate Judiciary Chair Dick Durbin (D-IL)

The *STOP CSAM Act* is a comprehensive response to online child sexual exploitation, which continues to increase at an alarming rate. From March 2009 to February 2022, the number of victims identified in child sexual abuse material (CSAM) rose ***almost ten-fold***, from 2,172 victims to over 21,413 victims. From 2012 to 2022, the volume of reports to the National Center for Missing & Exploited Children's CyberTipline concerning child sexual exploitation increased by ***a factor of 77*** (415,650 reports to over 32 million reports). To combat this horrific crime, the legislation takes a three-pronged approach that supports victims, promotes accountability and transparency by the tech industry, and ensures that offenders will receive sentences that reflect the severity of their crimes.

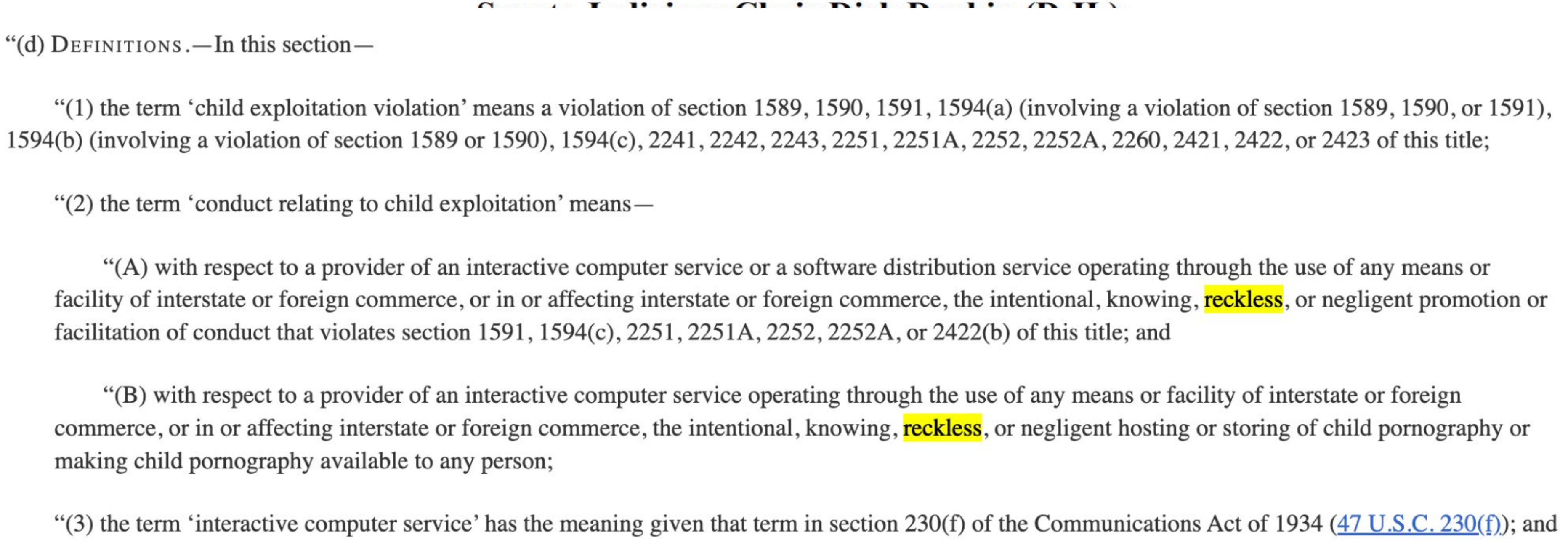
Child Victim Protection Measures

Mandatory child abuse reporting. The bill closes a reporting gap and creates a national safety net by ensuring that child-serving organizations that have 501(c)(3) tax-exempt status or that receive federal grants of more than $10,000 within a year report suspected child abuse to law enforcement.

Expanded protections for child victims and witnesses in federal court. The bill makes various

STOP CSAM Act of 2023

Senate Judiciary Chair Dick Durbin (D-IL)



"(d) DEFINITIONS.—In this section—

"(1) the term 'child exploitation violation' means a violation of section 1589, 1590, 1591, 1594(a) (involving a violation of section 1589, 1590, or 1591), 1594(b) (involving a violation of section 1589 or 1590), 1594(c), 2241, 2242, 2243, 2251, 2251A, 2252, 2252A, 2260, 2421, 2422, or 2423 of this title;

"(2) the term 'conduct relating to child exploitation' means—

"(A) with respect to a provider of an interactive computer service or a software distribution service operating through the use of any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, the intentional, knowing, reckless, or negligent promotion or facilitation of conduct that violates section 1591, 1594(c), 2251, 2251A, 2252, 2252A, or 2422(b) of this title; and

"(B) with respect to a provider of an interactive computer service operating through the use of any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, the intentional, knowing, reckless, or negligent hosting or storing of child pornography or making child pornography available to any person;

"(3) the term 'interactive computer service' has the meaning given that term in section 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f)); and

ensuring that child-serving organizations that have 501(c)(3) tax-exempt status or that receive federal grants of more than $10,000 within a year report suspected child abuse to law enforcement.

Expanded protections for child victims and witnesses in federal court. The bill makes various

Course Learning Goals

- Know and understand the fundamental tools that secure the modern internet
- Educated guess as to **WHY** components of secure protocol are there
- Develop/deepen adversarial thinking
- Strengthening independent learning skills

Final Logistics

- Final will be at time scheduled by the registrar
  - Friday May 12, 6:00pm-8:00pm
- Format
  - True/False + Justify
  - Open Answer (short/long)
- Cheat Sheet
  - 5 Pages. Double sided if you like. Welcome to print/handwrite/anything you want as long as it's not internet connected
  - Turn it in at the end for 5% bonus points on exam

Course Outline

Part 1: When Networking Protocols Go Wrong

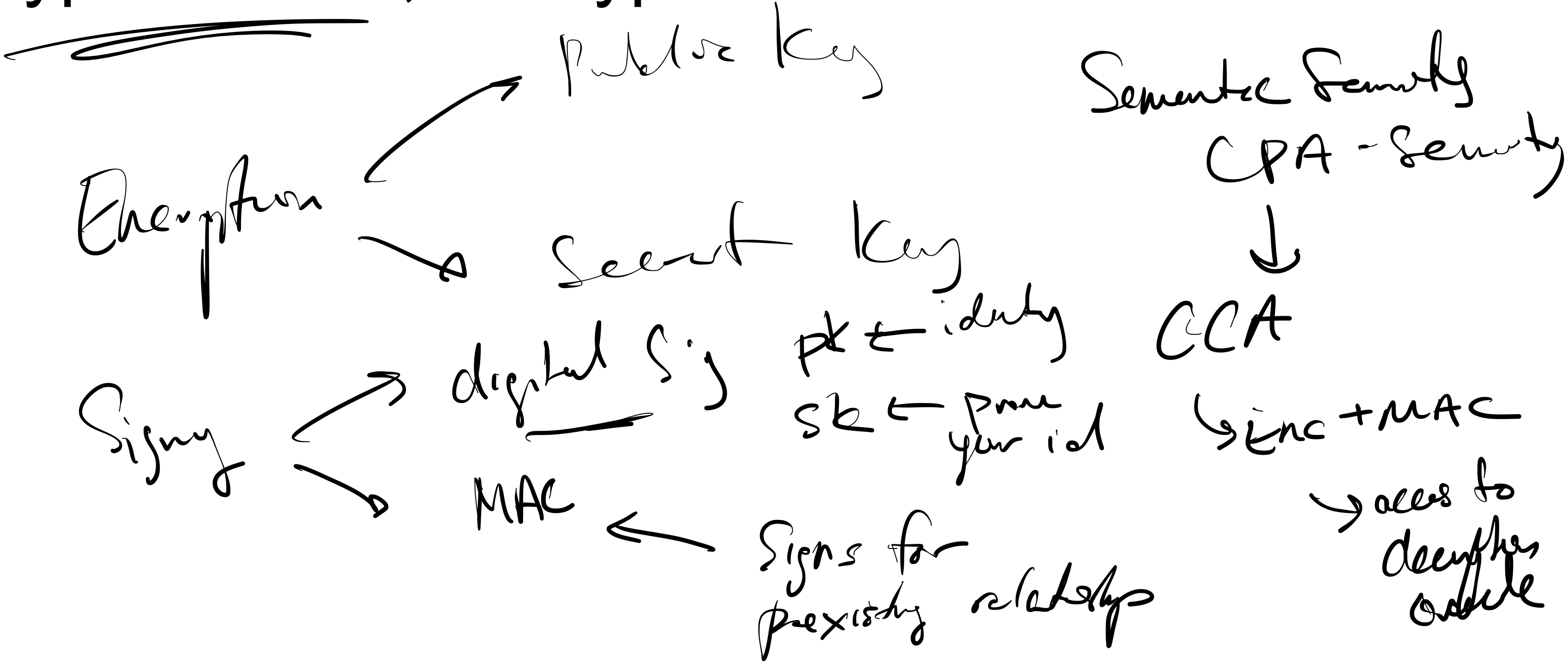
(Or, “Wait… what if someone doesn’t play nice?!?”)

- ARP, DNS, BGP, TLS.

Part 2: Privacy on the web

- Censorship Resistance (Tor, Accessing Tor)
- A little bit of secure messaging

Crypto Basics, Encrypted Email



Encryption → Public Key

Encryption → Secret Key

Signing → digital Sig

Signing → MAC

pk ← identity

sk ← prove your id

MAC ← Signs for preexisting relationship

Semantic Security

CPA-Security

↓

CCA

↳ Enc + MAC

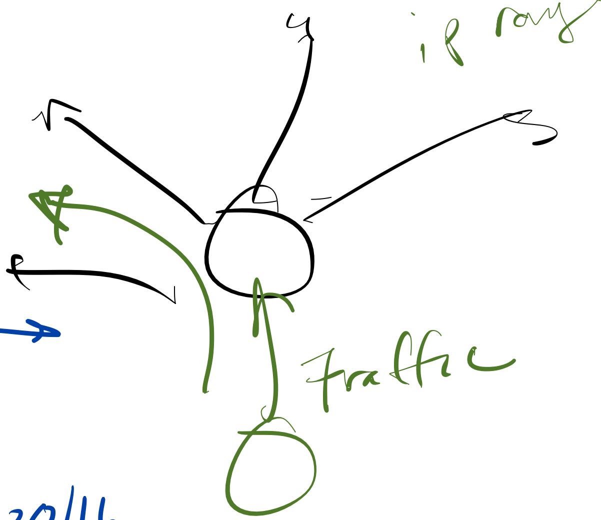
→ access to decryption oracle

ARP

→ ramifications of Γ_{yy}.

BGP, BGP Hijacking, RPKI, BGPSec

Hierarchical delegation of ip ranges



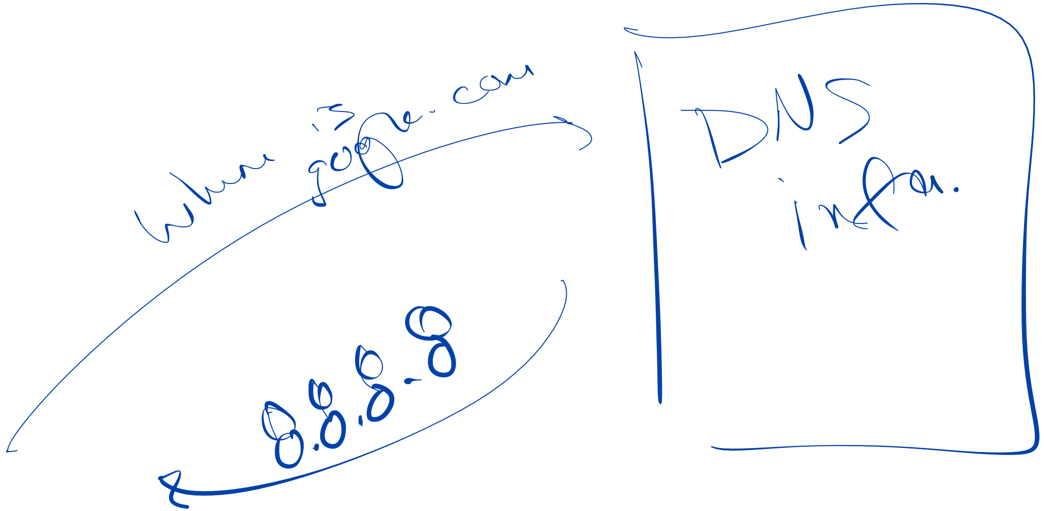
128.220.150.7

Hey! i know a path to 128.220/16

(D)DoS

UDP Spoofing

DNS/DNSSec

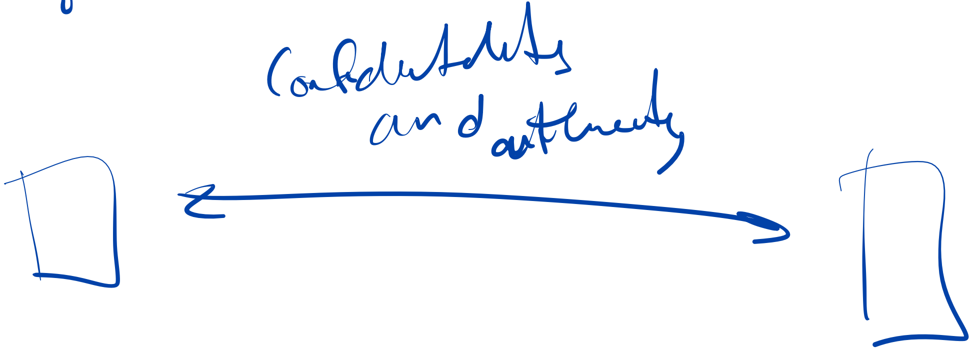


SSH

Enc → confidentiality (1) Key Encapsulation

(2) actually Enc

Signature → Prove our identity



TLS1.2, TLS 1.3 (Forward Secrecy)

multiple key Agreement protocols

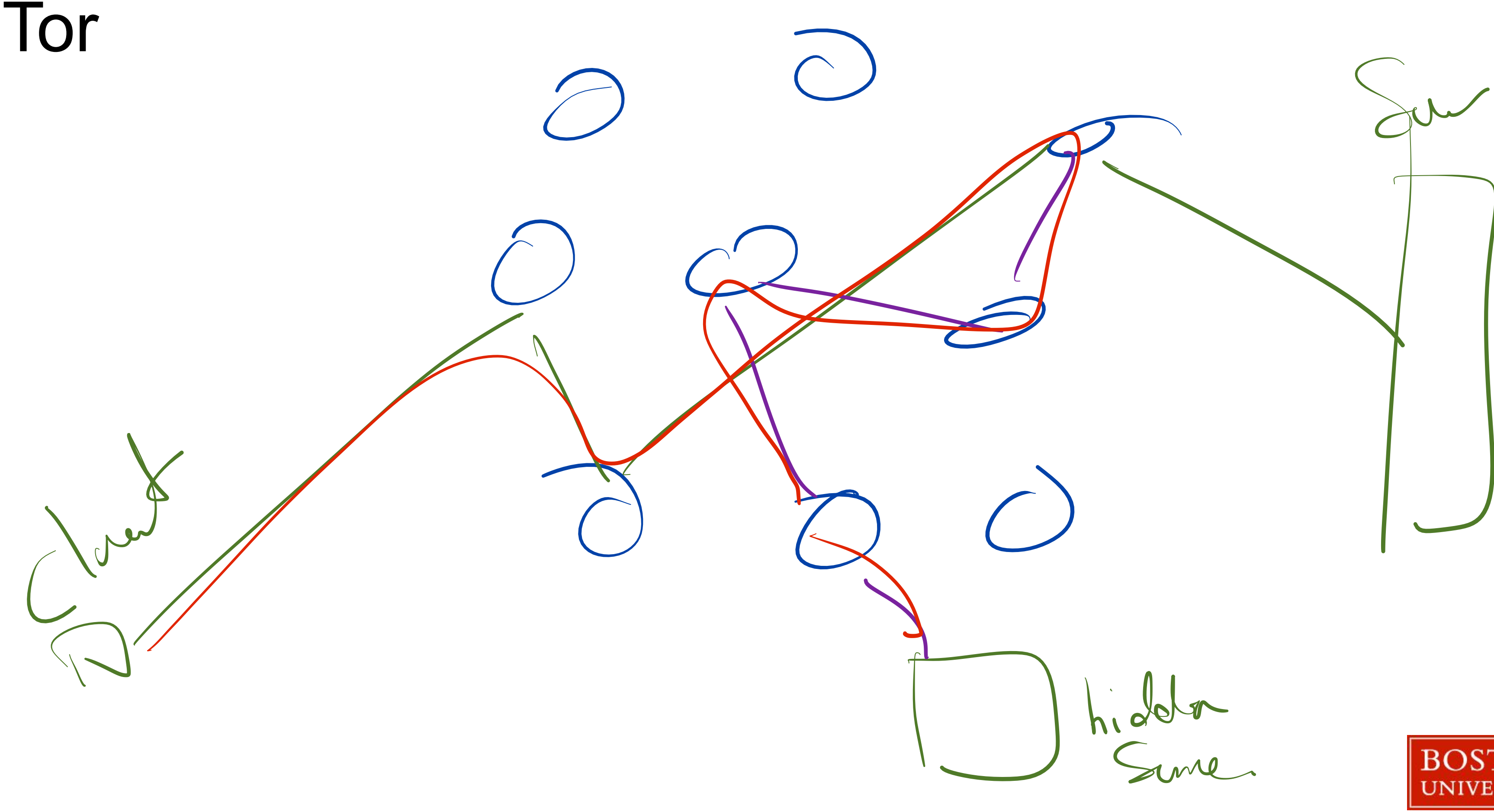
Replay attack

KE ← obvious try to do

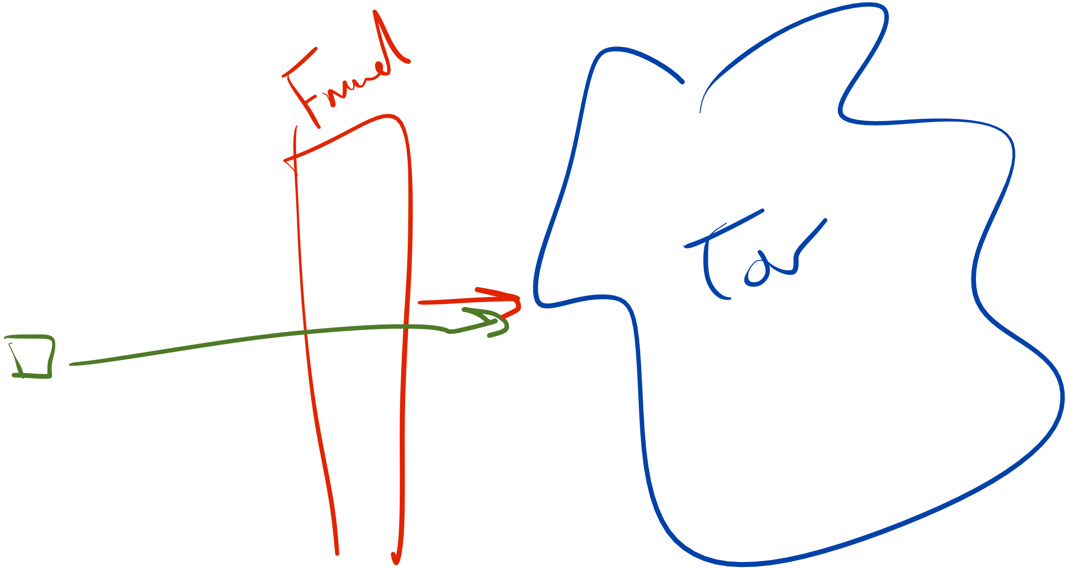
Static DH ← g^b ← b is long term

Ephemeral DH

Tor

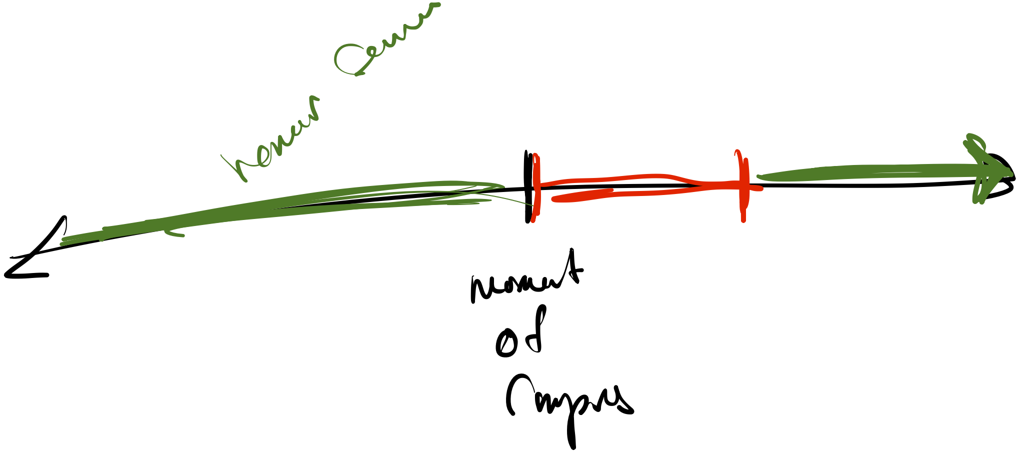


Censorship Circumvention (Pluggable Transport)



Post Compromise Security

Opaq + Password


Never Secure
moment of Compromise