self-censorship as consequence

tower operator with "anonymous power"

constant visibility

Panopticism:
more supervision = more security

internet, phone, CCTV

mass (all) surveilence

targeted (suspects)

spyware

not the norm, but neccessary

EU ePrivacy Regulation

European Convention of Human Rights

Data Retention Directive

Legal

DSGVO

Socialogical Aspects

Political & Legal Aspects

Privacy

Universal Human Right

right to be left alone

right to decide what information to share

Surveilence - Political

Censorship

Conformity

Panopticism

Paternalism

Technical Aspects

Snowdens Revelations

PRISM

direct access to data

targets data at rest

internet communication

X-KEY-SCORE (analytical database)

Metadata

buffered for 30 days

no direct access needed

Immersion: visualization of metadata

Social Snapshots & Social Graphs

"Profile-cloning" Attacks

User Profiling

"Cross-Network-Cloning"

Social Engineering

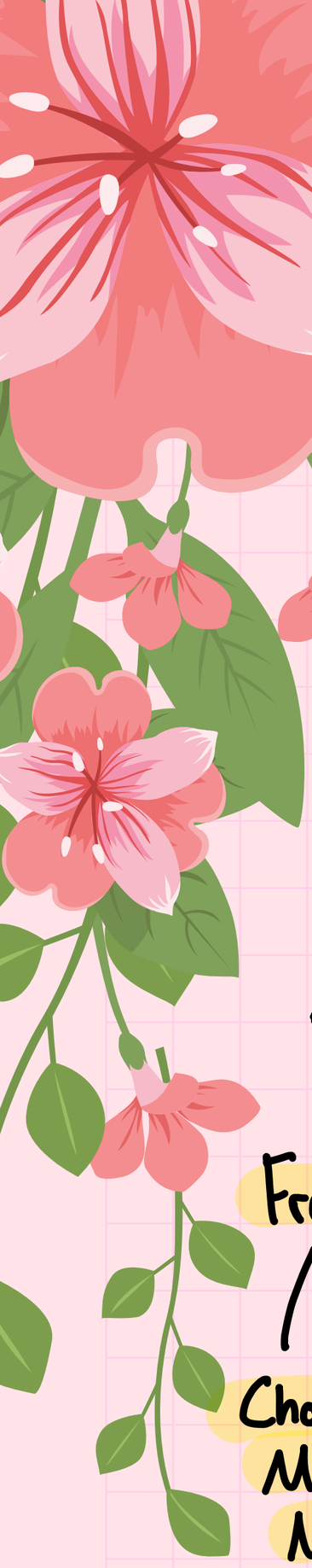
password questions

answers found on socials

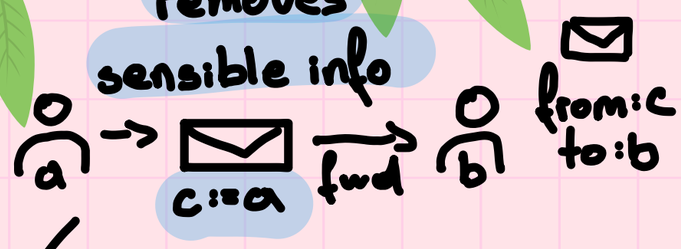
context-aware spam

social phishing

OSINT



removes sensible info



encrypted traffic to remailer

Cypherpunk

implements CM

Mixmaster

unlinkability

Remailer

TLS

Mixminion

mixes order of messages

pooling

batching

Chaum-Mix

message chunking

Problem: Database with links

Penet Remailer

for message-based systems

DoS protection

slower, asynchronous transmission acceptable

High-Latency

File-Sharing

P2P

Freenet

censorship resistence

unidentifiable within anonymity set (peer group)

pseudo-anonymity (fake names)

Anonymity

unlinkability (e.g. via Tor)

Chaum Mix Nets

GUID

unob-servability

sender/ recipient anon.

Opennet & Darknet Mode

Low-Latency

relationship anon. (no link between messages & users)

protocol-independent

VPNs

supports encryption protocols

linkable via. provider

higher interactivity, little delay

Mix Networks

Proxies

protocol dependent: single point of failure

possible deanonymization via JS/Java

Onion Routing (Cascade of ORs)

Garlic Routing

Experimental Systems

(p^5)

Message bundling

Symmetric + Asymmetric Encryption

P2P Personal Privacy Protocol (Broadcast Rings)

(I2P)

Invisible Internet Project

for secure channels, long messages

collisions, disruptions, complexity

creates local proxy

Applications:
- FileSharing
- E-Mail
- Messaging
- Publishing

transmit any type of info

DC-Nets

strong anonymity

Concepts & Techniques

- DNS Filtering
  - Block
  - Modify
  - Redirect
- BGP Hijacking
- DoS Attacks
  - Disconnect
- Network & Routing
- IP Blocking
- Connection Reset
- JS-Injection
- URL Filter
- Active SSL MITM
- Direct Censorship (How)
  - Fingerprinting
    - TLS
      - SNI-Blocking
    - Fingerprinting (What)
      - Great Firewall of China vs. Tor

Block Tor -> Mirrors -> Block Mirrors -> Bridges -> Count & Block Bridges -> Secret unknown bridges -> DPI -> Pluggable Transports -> Probing against PT -> PT-design against probing

Detection & Measurement

- Who
  - RSF
  - OONI (HTTP, DNS,...)
  - Ripe Atlas
  - RTR (AT)
  - Users
    - Freedom on the Net
      - Access Restriction
      - Content Restriction
    - Tor Metrics
      - User Location

Censorship

- DNS tampering
- DPI
- Catalonia
  - HTTP block
- since 2015
- Austria
  - DNS-based
- Google DNS hijacking
  - Turkey (DNS)

Censorship Events Worldwide

Countermeasures & Circumvention

- Domain Fronting
- Alternative DNS Server
- Snow-flake
- Plugabble Transports
- Meek
- VPN
- Tor

Large-scale use of TCP RST

DPI on encryption

Great Firewall of China

- huge word list
- 350 processes
- Tor bridges semi-blocked
- prevents open resolvers

Secure Messaging

Message-based Protocols

PGP
- En-/Decryption
- Hex Hash
- GPG
- Signing
- Authentification
- Hybrid Encryption
- no plausible deniability
- no forward secrecy

EFAIL
- direct exfiltration
- multi-part email

S/MIME
- Hirarchical PKI

OTR
- Asynchronous
- Internet Chats
- Encryption
- Authentication
- Perfect Forward Secrecy
- Plausible Deniability

Session-based Protocols

- Ephe-meral Diffie-Hellmann keys (AES)

Anonymity & Secure Messaging

- metadata leaked
- traffic analysis

Tor Messenger

Ricochet

ChatSecure

Secure Mobile Messaging

- Design Documentation
- mostly TLS
- provider can read & share
- Client-Server Encryption
- Code Audit
- only clients can decrypt
- End-to-End
- Contact Verification
- Forward Secrecy
- Open Source
- Ephemeral Messaging
- deceptive marketing
- provider can read "deleted" messages

Matrix/Element
- for de-centralisation

Double Rachet Algorithm
- DH from OTR
- Symmetric key ratchet from SCIMP

Transport Layer Security

Cryptographic Primitives

- Symmetric Cryptography for transport
  - AES
- Authentication
  - RSA
- Integrity
  - SHA
- AEAD
- Key exchange
  - DHE
- Ciphersuites
- Forward Secrecy

Public Key Infrastructure (PKI)

- Chain of trust
  - sub-CA -> Root CA
- X.509
- NSS
- BoringSSL
- OpenSSL
- LibreSSL

Application of TLS

HTTPS

- Certificates
  - cost -> Let's Encrypt
- Adoption
- Bad Documentation
- Difficult Deployment
- Usability
- SSLTest
- Secure Deployment

Email

- POP, IMAP, SMTP
- STARTTLS
  - Opportunistic encryption

Improvements

- Logs
  - Certificate Transparency
    - Auditor
    - Monitor
- HTTPS Everywhere
- SSLTest
- Qualys
- MTA-STS
- DANE
- TLS 1.3
- Certification Authority Authorization
  - allows some CAs to issue Certs
- Pinning
  - Key Distribution Problem
  - (HPKP) HTTP Public Key Pinning
    - EOL
  - CA check
- (HSTS) HTTP Strict Transport Security
- Let's Encrypt
  - Easy TLS setup
  - ACME protocol
  - Certbot

Flaws

- DROWN
- POODLE
- FREAK
- SMACK
- RC_4 feasable
- STRIPTLS
- Weak keys
- Weak DH

Handshake protocol

- protocol independent
- Record protocol

The Onion Router (Tor)

Components & Techniques

- Cells
  - Control
    - create
    - padding
    - destroy
  - Relay
  - Link
- Tor Client
  - first relay
  - last relay
  - Thread Model
- Tor Relay
  - multiple keys
- Tor Circuit
- Directory Authority
  - 9 word-wide
- Anonimizes TCP Connections
- No P2P
- No UDP
- No steganography
- No cover traffic
- No protection
  - traffic confirmation attacks
  - Complex protocols
  - Layer & traffic
- Cryptography
  - SHA-256
  - AES in CTR-mode
  - DHE
  - TLS between relays
  - Forward Secrecy
- Heartbleed
  - OpenSSL
  - weak keys
  - zmap, masscan
- Cons
  - traffic detectable using deep packet inspection (DPI)
  - delay
- Pros
  - no single point of trust
  - Open Source
  - robust, well-established

Attacking & Using Tor

- BitTorrent
  - can de-anonymize
- traffic correlation for first and last relay
- RelayBandWidthRate
- Exit Policy
  - ORPort, DirPort
- MITM through exit relay
- HoneyConnector
- exit-map
- air-gapped machines
- .exe, .pdf, .zip = problematic
- Hosting
  - Bridges
  - PTs
    - obfsh
    - Snowflake
    - meek
- Using Tor
  - check signatures
  - GeoIP
  - TorPS (Path Sim)
  - Tor Simulators
    - e.g. Shadow

Onion Services

- bypass DPI & censors
- DoS protection
- TLS
- anonymous server & services
  - no geolocation
  - operates despite firewalls
  - Silkroad
  - base32
  - 16 characters 2-7, a-z
    - 56 chars
  - Freedom Hosting

Web Tracking

- First Parties
  - sell User Data
  - Misuse Security Bugs
- Third Parties
  - URL leak via Referrer
  - Advertisement
    - Ad Networks
    - Targeted Ads
    - Ad exchanges
  - Social Networks
    - Social Plugins
      - Share
      - Like
      - Add
      - SSO
    - Mozilla Lightbeam
  - is first party too
- Cross-Site-Linking
  - e.g. Profile Pictures
- Unique User Profiles
  - HTTP tracking cookie
- Finger-printing
  - HTML5 Canvas
  - no cookie
- Super-cookie
  - alt. storage location
- (DNT) Do Not Track
  - HTTP Header
    - Opt-Out
      - persistent oo cookie
    - Global Privacy Control (GPC)

Network Layer Tracking

- (TLS) DoT
- (HTTP) DoH
- DNS Leaks
- Monitor/Censor through DPI
- HTTP Leaks

Web Privacy

Tracking Protection

- Browser
  - Google Chrome
    - First-Party Tracking
    - Intelligent Tracking Prevention
      - 1. Party after 7 days
      - Purge cookies
      - 3. Party after 30 days
  - Apple Safari
  - Brave
    - Tracking & Fingerprinting Protection
    - Tor-browser tabs
  - Mozilla Firefox
    - Multi-Account Containers
    - Tracking Prevention
      - Disconnet Ruleset
      - Seperate Cookie Context
- Browser-Settings
  - Deletion of Cookies
  - Private Mode
- Extensions
  - uBlock
  - ABP
  - Ghostery
  - Privacy Badger
  - Disconnect.me
- Privacy Respecting Ad Ecosystem
- Mobile & "Smart" Devices
  - sensitive Metadata
  - pi-hole
  - OS-background-services
  - Cross-Device-Tracking
  - DNS blocking

Virtual Private Networks (VPNs)

Technologies

Wireguard

- easy, fast
- UDP-only
- part of linux kernel
- Cryptography
  - ChaCha20 (encryption)
  - Poly1305 (me)
  - (Hash) Blake2s
- X25519 (ke)

IPSec

- Authentication Header (AH)
- Modes
  - Transport
  - Tunnel
    - Packet-in-Packet
      - Destination encrypted
- (ESP) Encapsuling Security Protocol
- (SA) Security Association
  - key exchange, e.g. IKEv2

applications

- user-to-site
- site-to-site
- split tunneling

TLS-based

- OpenVPN
  - endpoints always online
    - prone to attacks

trust-based "no logging"

Alternatives

- remote IP
  - SSH tunnel
- Starlink
- private APN
- private 5G networks
- Layer 2, over wi-fi
  - 5GHz, 60GHz
  - point-to-point links
    - line-of-sight necessary
- MLPS
- MACsec
  - for local networks
  - AES-GCM-128