Towards a systematic analysis of threats and requirements for private messaging: the case of emailing and instant messaging

Dr. Iraklis Symeonidis
Post-doctoral researcher
SnT - APSIA
University of Luxembourg

p≡p

Singapore
18 November 2019

UNIVERSITÉ DU LUXEMBOURG

Keywords

Systematic analysis

Threats and requirements

Aim of this presentation:

- Stimulate discussions for feedback on our I-D
- Call for contributions

Security and privacy

Private messaging: email and instant messaging

Co-authors Information

Bernie Hoeneisen
Nana Karltetter

Full time post-doctoral researcher
SnT / APSIA
University of Luxembourg

Affiliated post-doctoral researcher
imec-COSIC, KU Leuven

PRIVATE MESSAGE: EMAIL AND INSTANT MESSAGING

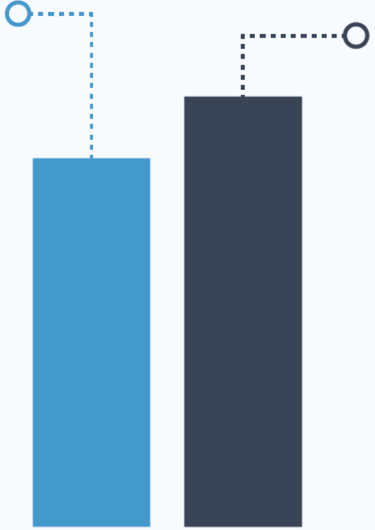
STILL A RELEVANT PROBLEM?

Email in numbers

Oberlo

The Widespread Usage of Email

In 2017, global email users amounted to **3.7 billion** users
(Statista, 2018)

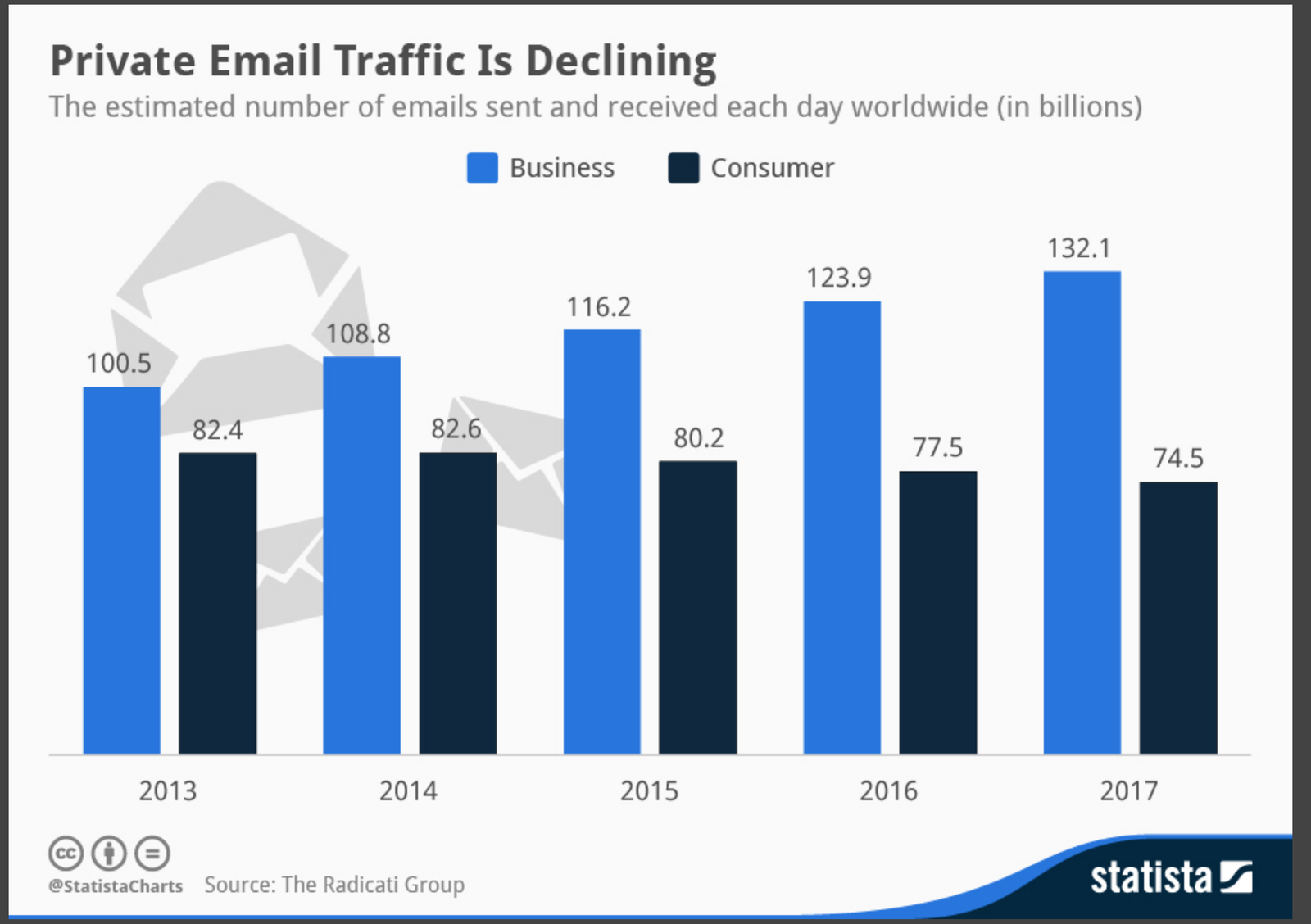


In 2022, this figure is set to grow to **4.3 billion** users
(Statista, 2018)

That's half of the world's population

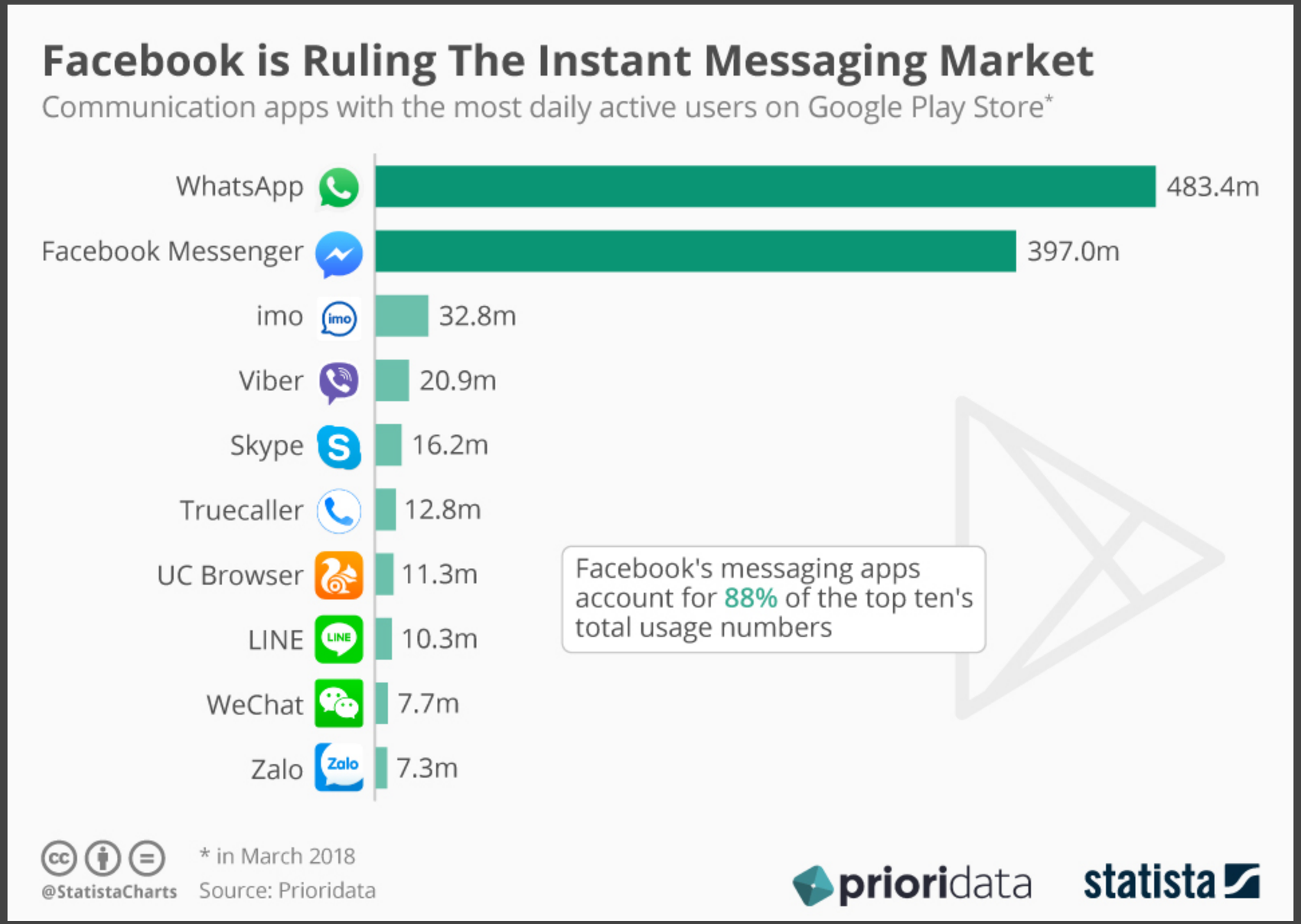
Credits: oberlo.com

Email in numbers



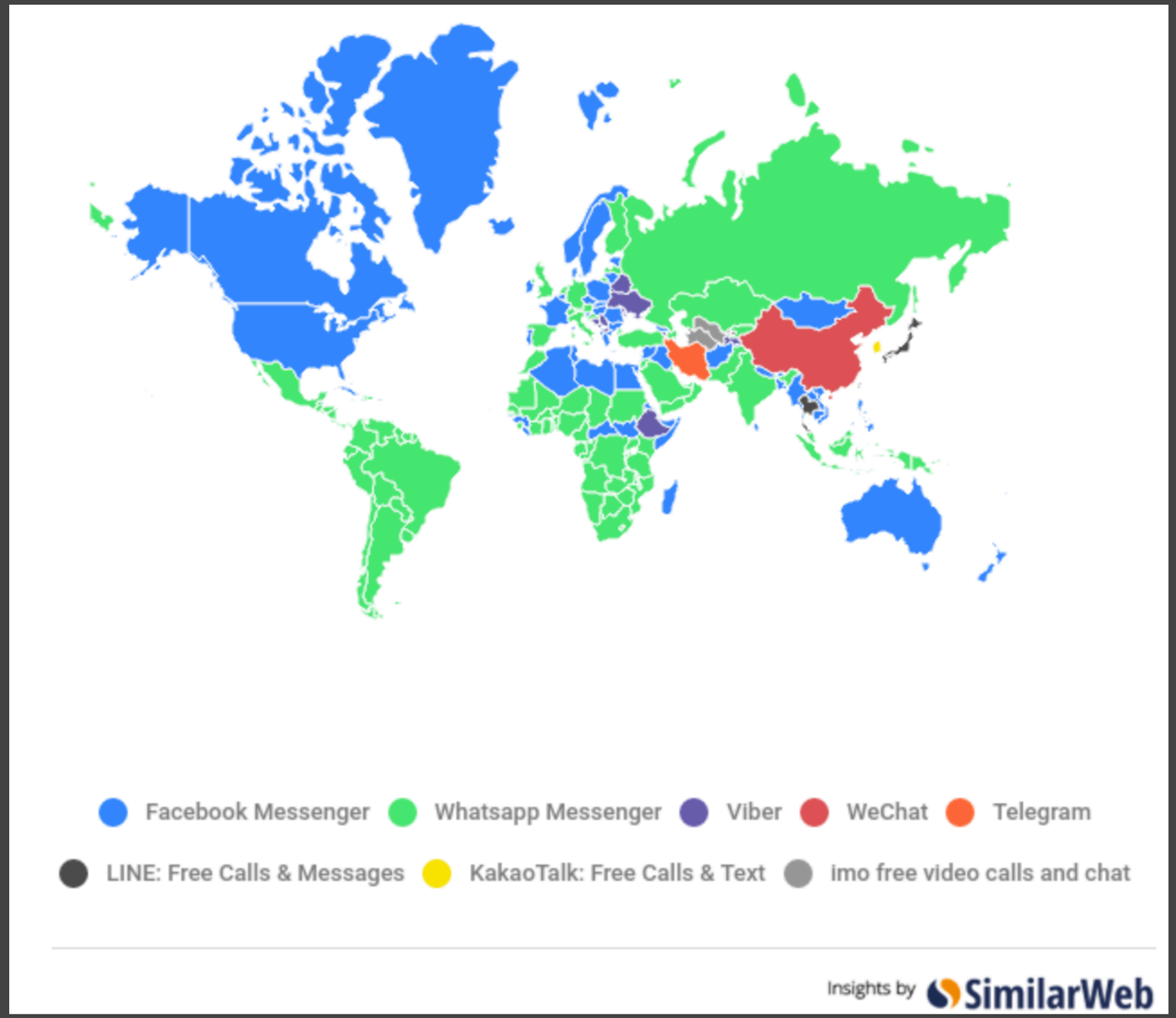
Credits: statista.com

Instant messaging in numbers



Credits: statista.com

Most popular IM app in every country (Android app store'17)

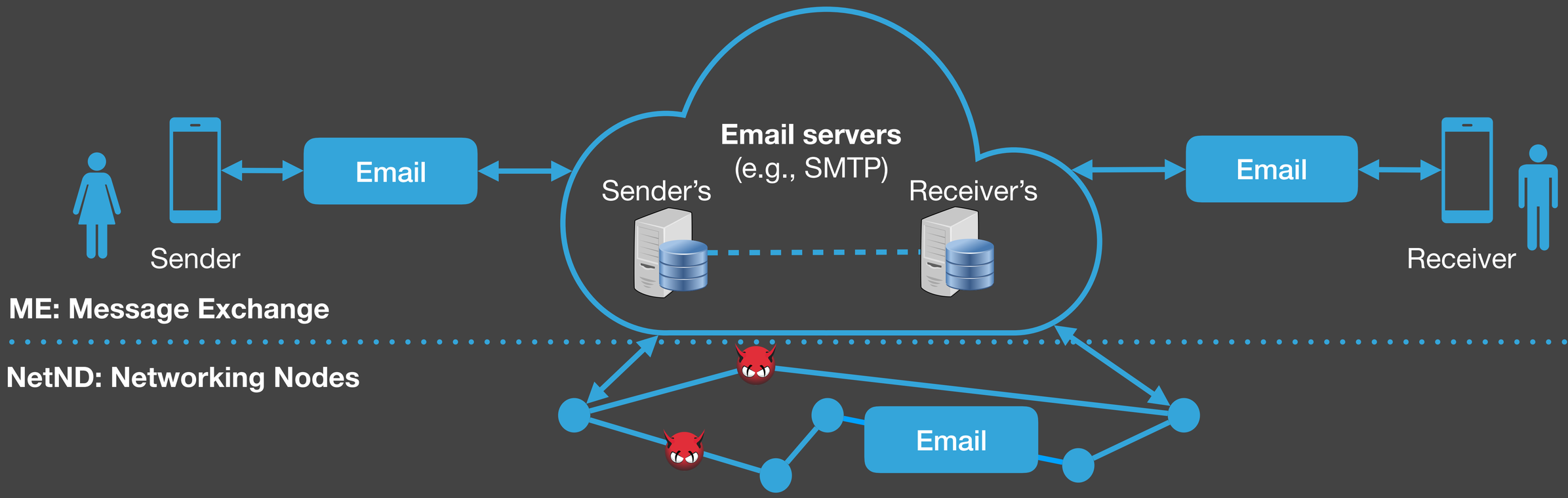


Credits: www.similarweb.com

PRIVATE MESSAGE: EMAIL AND INSTANT MESSAGING

DO WE HAVE A SYSTEMATIC APPROACH FO SECURITY AND PRIVACY CHALLENGES?

Security and privacy threats: running examples

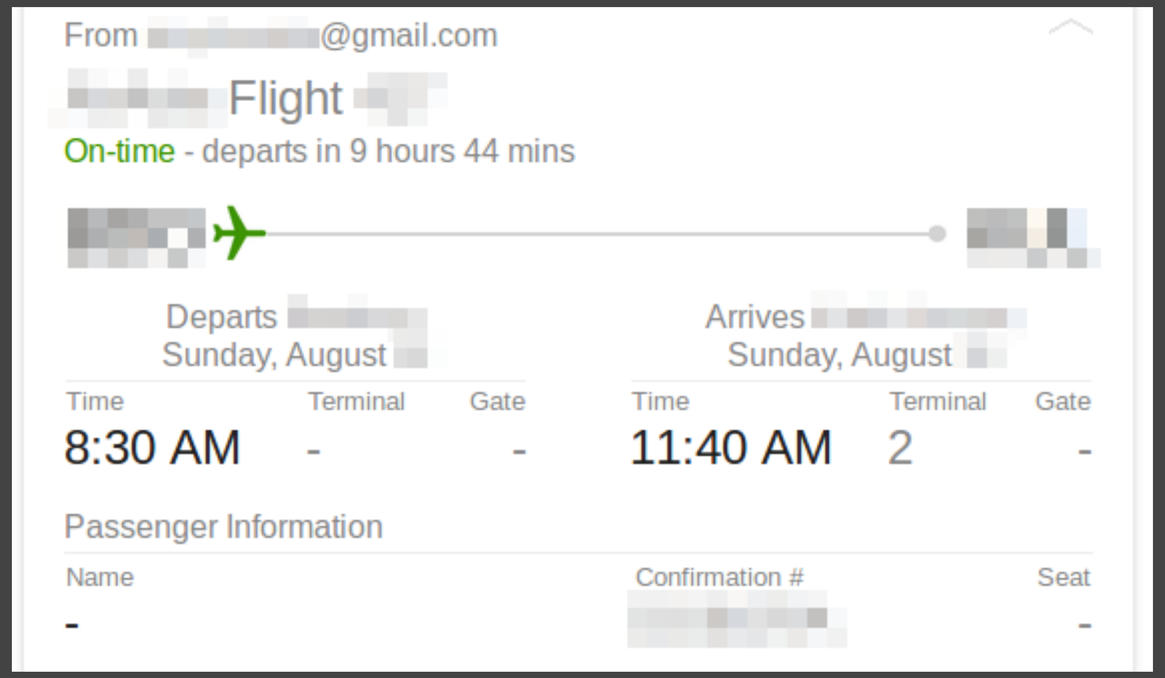


- **SMTP**: No build in security

- MiTM attacks were trivial

Security and privacy threats: running examples

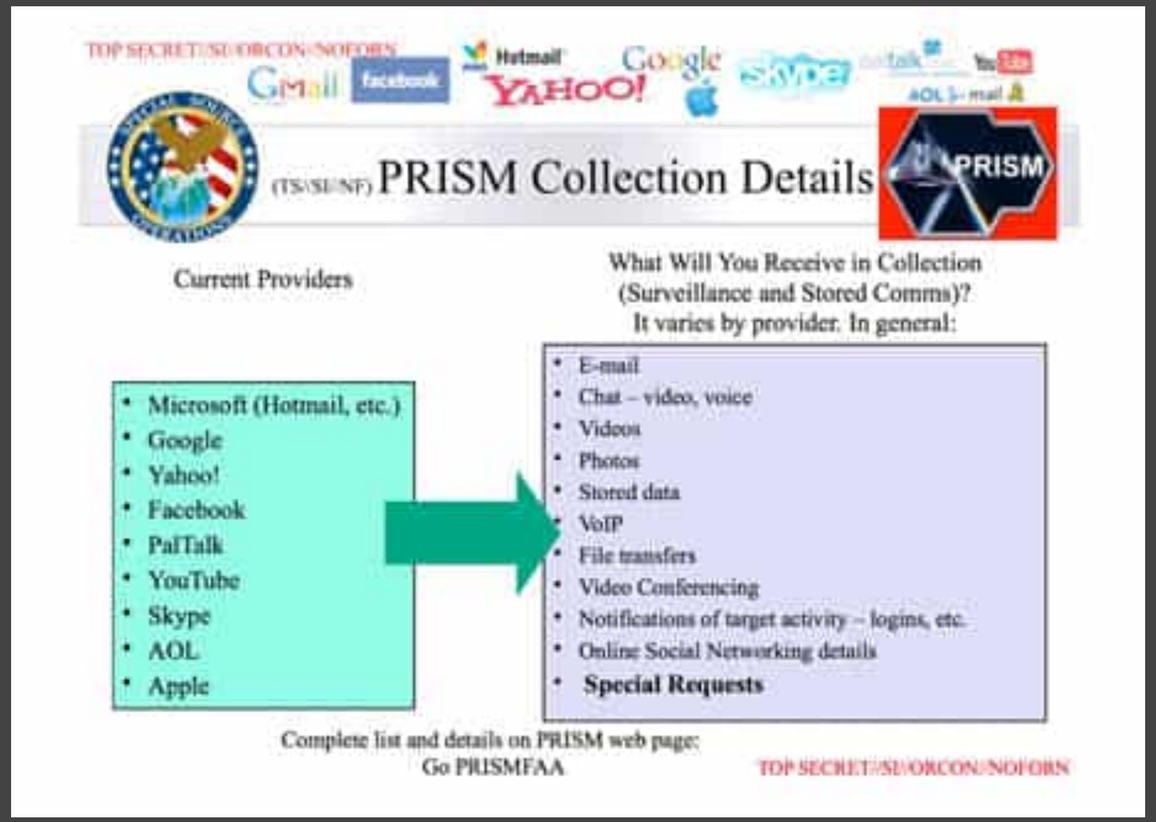
Gmail analytics



Credits: Google

- Client-server encryption

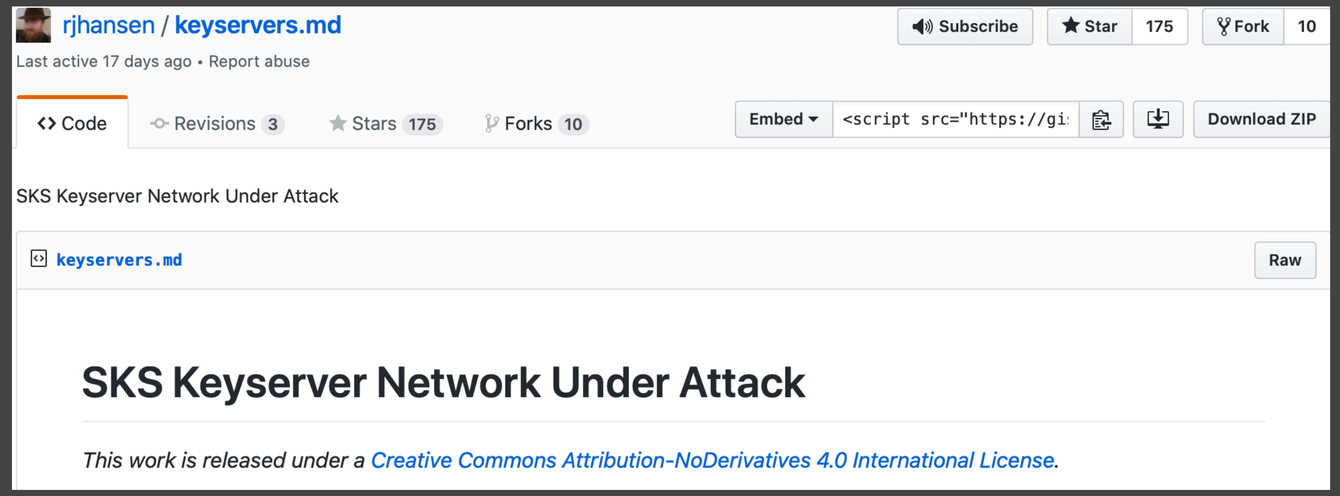
Snowden revelations 2013



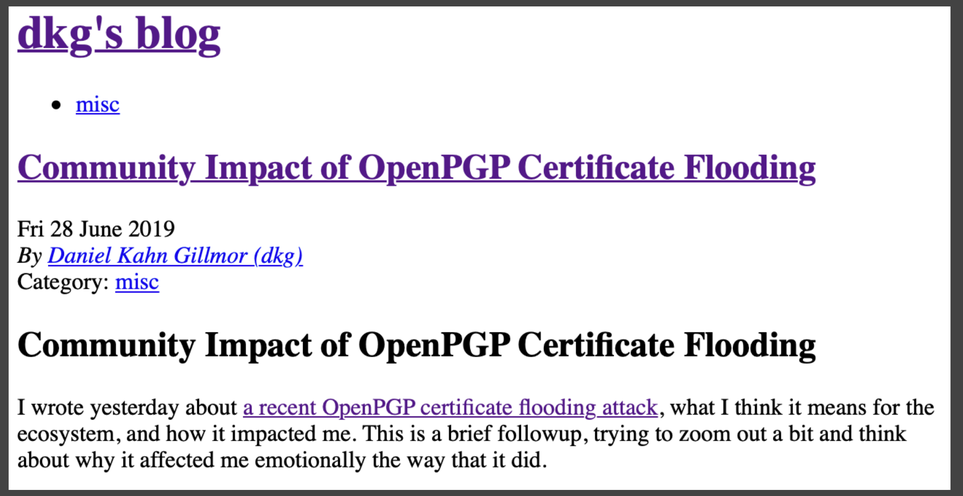
Credits: Guardian

- Untrusted communication servers

Security and privacy threats: running examples



Credits: https://gist.github.com



Credits: https://dkg.fifthhorseman.net

Synchronizing Key Server (SKS)

- Signing certificates to enhance trust

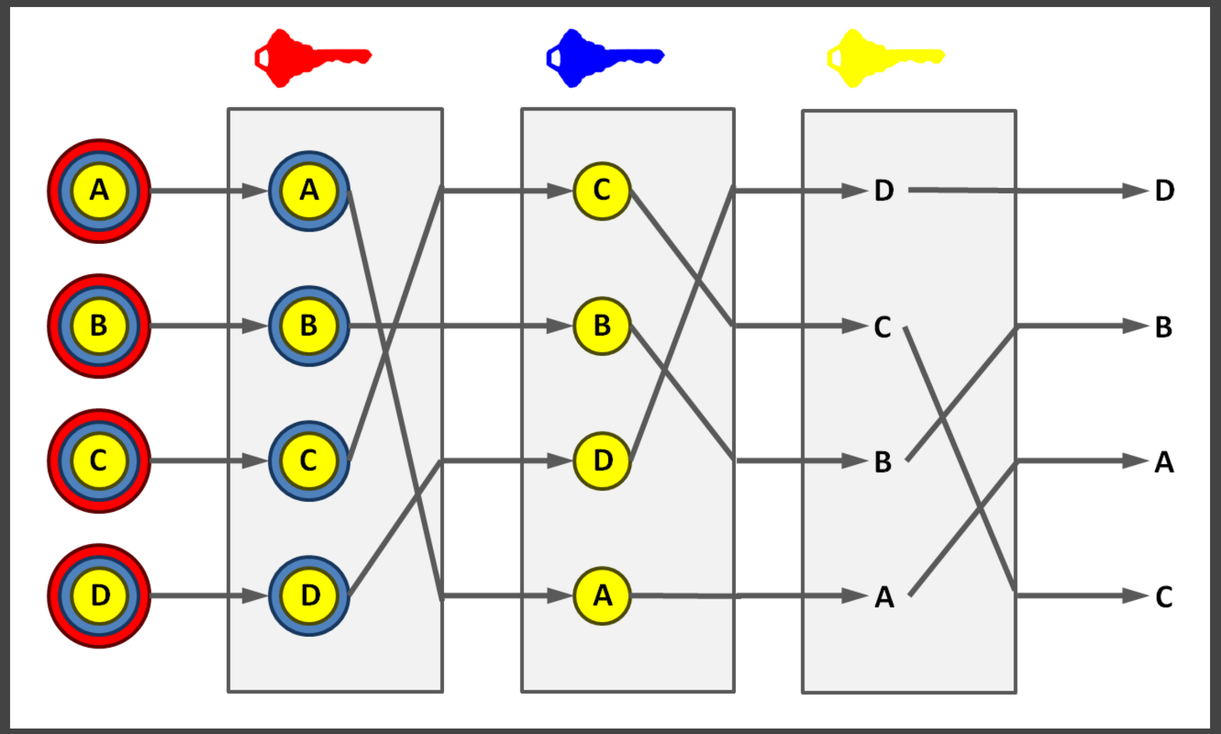
Certificate poisoning (June'19):

- **Spamming**: rogue signing legitimate certificate - an increase of the certificate size in the Key server - no upper limit in the protocol
- **Aim**: make GnuPG/Enigmail to stop working/make also certificate useless (single cert:~150k signatures/cert. ~45Mb/cert)
- **Target**: Robert J. Hansen and Daniel Kahn Gillmor - contributors in the OpenPGP community

Security and privacy threats: running examples

Michael Hayden
General and former director NSA/CIA'14

Credits: www.youtube.com

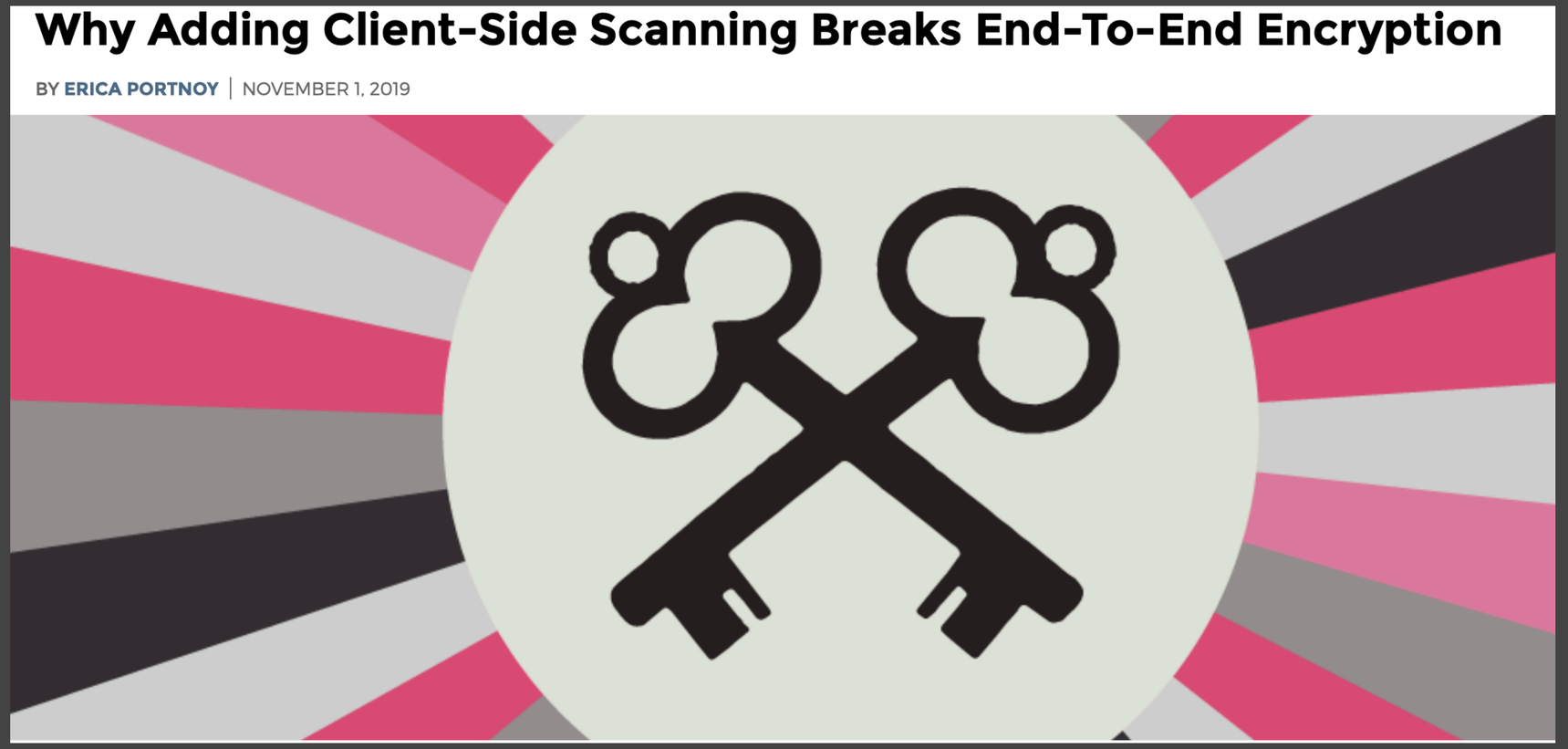


Credits: en.wikipedia.org/

Panoramix

Credits: panoramix-project.eu

Information Disclosure



Credits: eff.org

- Scanning pictures before sending via private messaging systems

- You cannot check the DB with hashes
- Why not that apply for text?

RELATED WORK AND OBJECTIVES?

Related work

- Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg, Matthew Smith, **SoK: Secure Messaging,** IEEE Symposium on Security and Privacy 2015: 232-249
- Jeremy Clark, Paul C. van Oorschot, Scott Ruoti, Kent E. Seamons, Daniel Zappala: **Securing Email,** CoRR abs/1804.07706 (2018) 2017
- Ksenia Ermoshina, Francesca Musiani, Harry Halpin, **End-to-End Encrypted Messaging Protocols: An Overview,** INSCI 2016: 244-254
- Fateme Shirazi, M Simeonovski, MR Asghar, M Backes, Claudia Diaz, **A survey on routing in anonymous communication protocols**, ACM Computing Surveys (CSUR) 51 (3), 39

State of the art

ELECTRONIC FRONTIER FOUNDATION

Secure Messaging Scorecard

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
AIM	✓	⊘	⊘	⊘	⊘	⊘	⊘
BlackBerry Messenger	✓	⊘	⊘	⊘	⊘	⊘	⊘

- List of apps + security design features

- Limited categories
- Obsolate
- Only for existing apps

Aim of I-D

Aim of I-D: provide methodology/guide for
- Assessing existing systems
- Designing new private messaging systems

Dimensions/challenges:
- **Technical threats**: security and privacy by design
- **User threats:** backdoors

- As a basis for private messaging standard in a later face (good fit for IETF)
- PEARG to consider adapting this I-D as a WG item (suggestion)

I-D: objectives

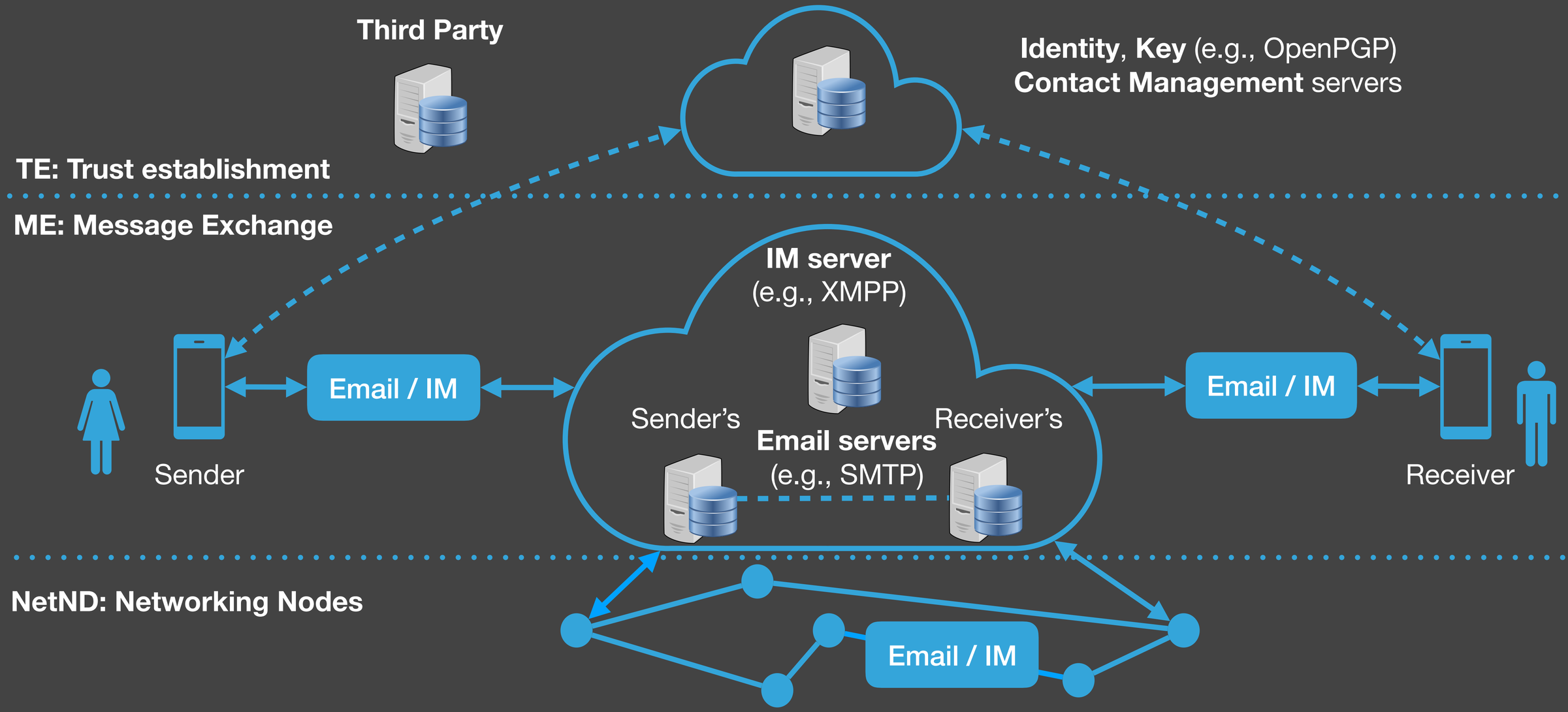
- System model:
  - Entities, functionalities
- Adversarial model:
  - Adversaries / adversarial type
- Classes of threats:
  - Technological / user
- Classes of requirements

- Risk - assessment for selection of threats
  - Define risk and evaluation?
- Primitives (crypto) to mitigate threats / minimize the risk

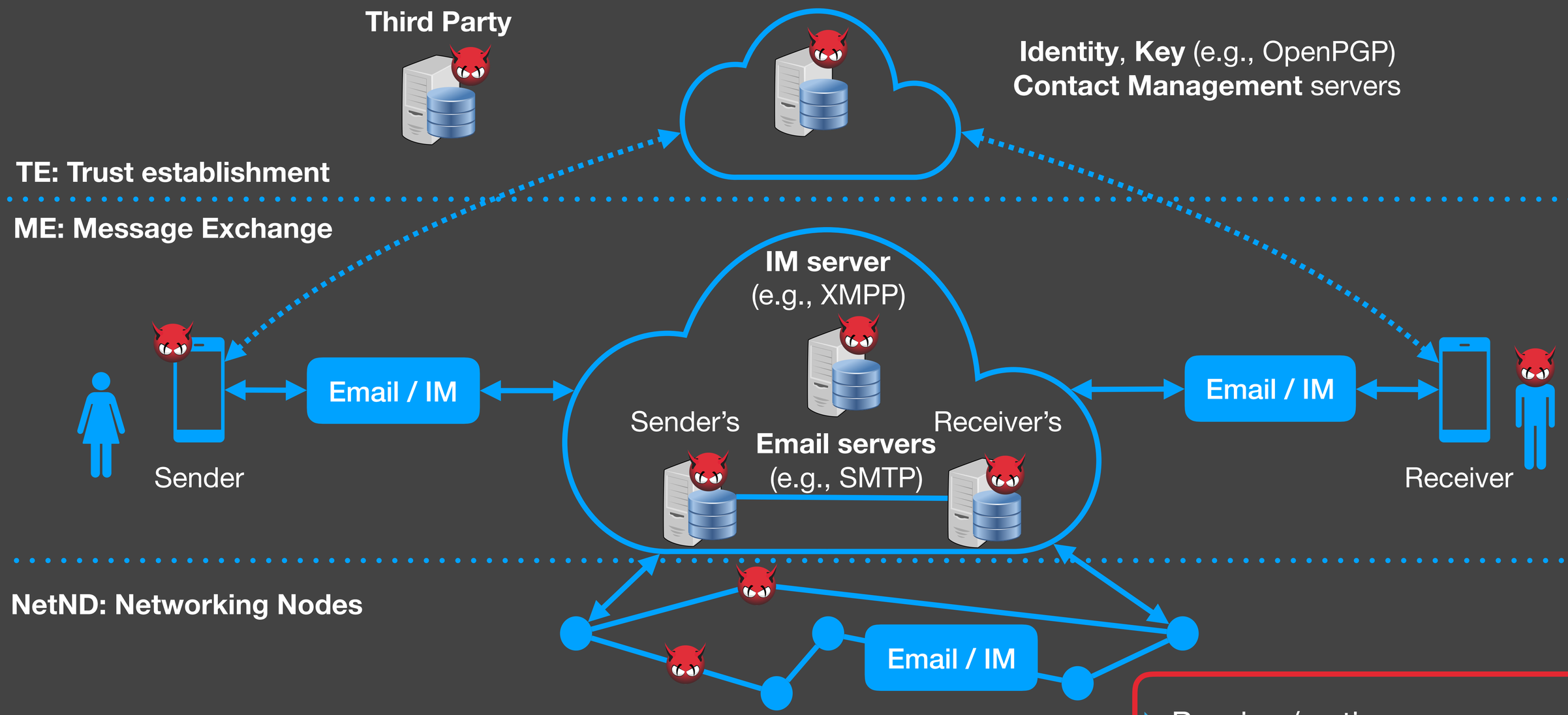
PRIVATE EMAILING AND INSTANT MESSAGING

THREATS AND REQUIREMENTS?

System model: Email and IM



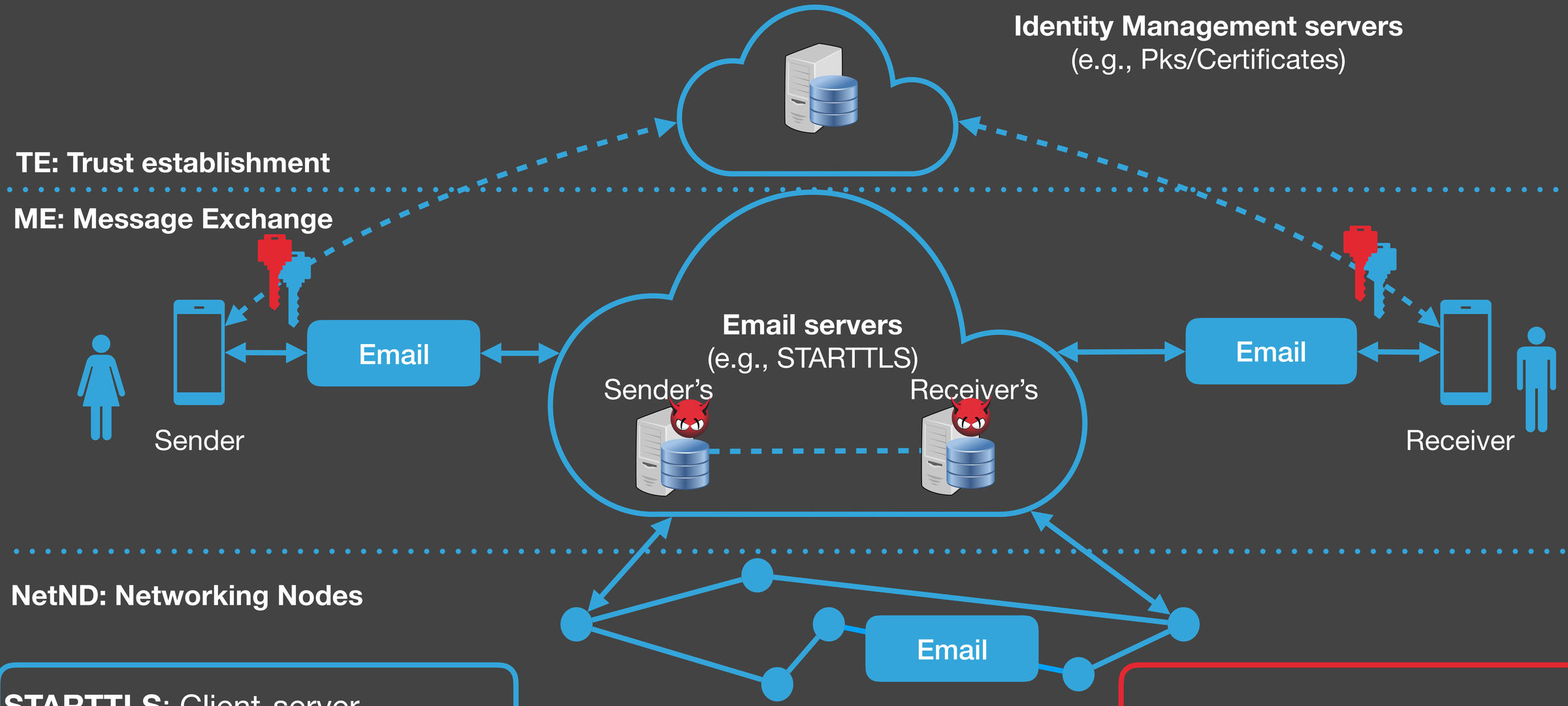
Adversaries and adversarial model



Secure and privacy enhancing emailing (challenges)

Security Threats	Sec. Requirements	Privacy Threats	Privacy Requirements
(S)poofing	Entity Authentication	(L)inkability	Unlinkability
(T)ampering	Data Authentication	(I)dentifiability	Anonymity / Pseudonymity
(R)epudiation	Non-Repudiation	Non-(R)epudiation	Plausible Deniability
(I)nformation Disclosure	Confidentiality	(D)etectability	Undetectability / Unbservability
(D)enial-of-Service	Availability	Information (D)isclosure	Confidentiality
(E)levation of Privilege	Authorisation	Privacy (I)nterdependence	Privacy Independence
		Policy and Consent (N)oncompliance	Policy and Consent Compliance

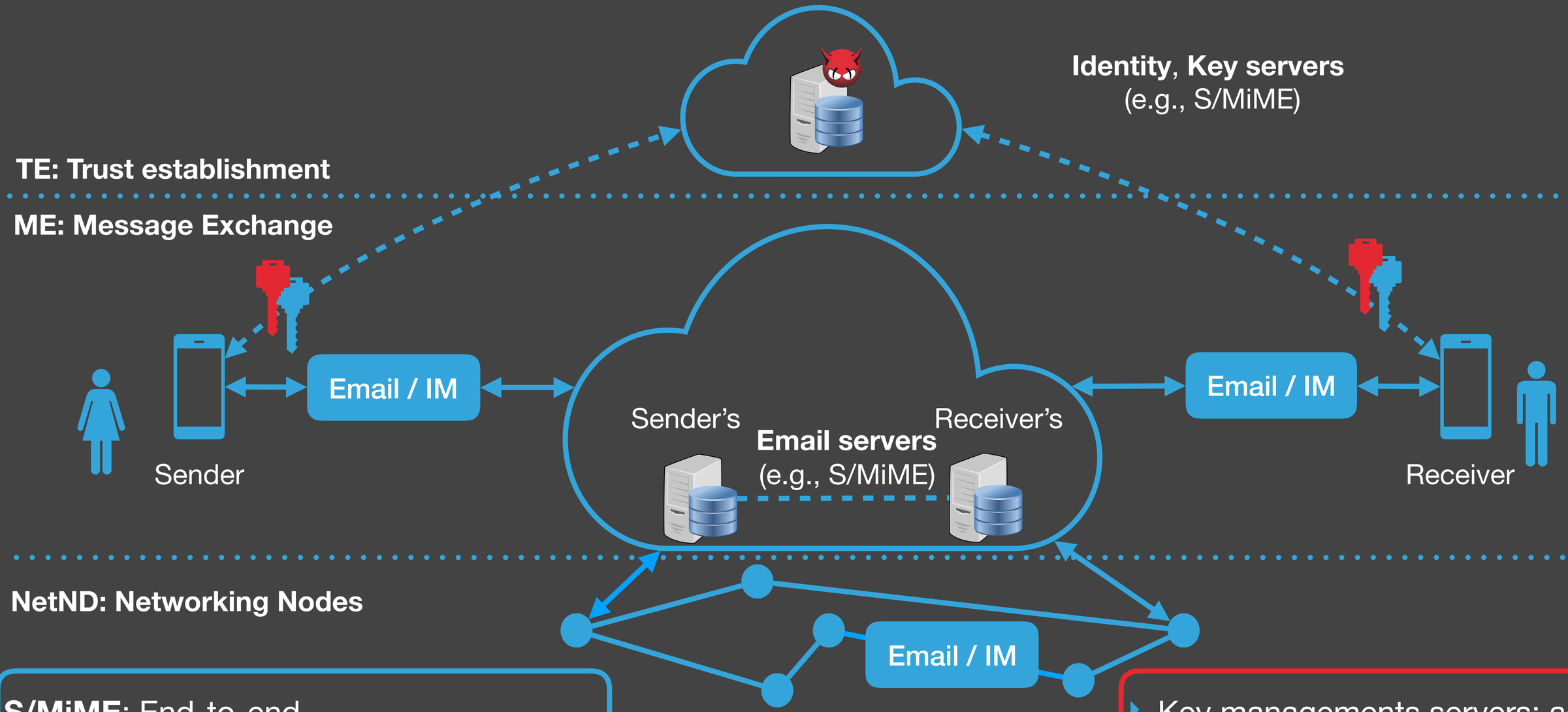
Case 1: STARTTLS and untrusted servers



STARTTLS: Client-server
- confidentiality, entity + data authentication

- **Email servers**: passive adversaries (no confidentiality)

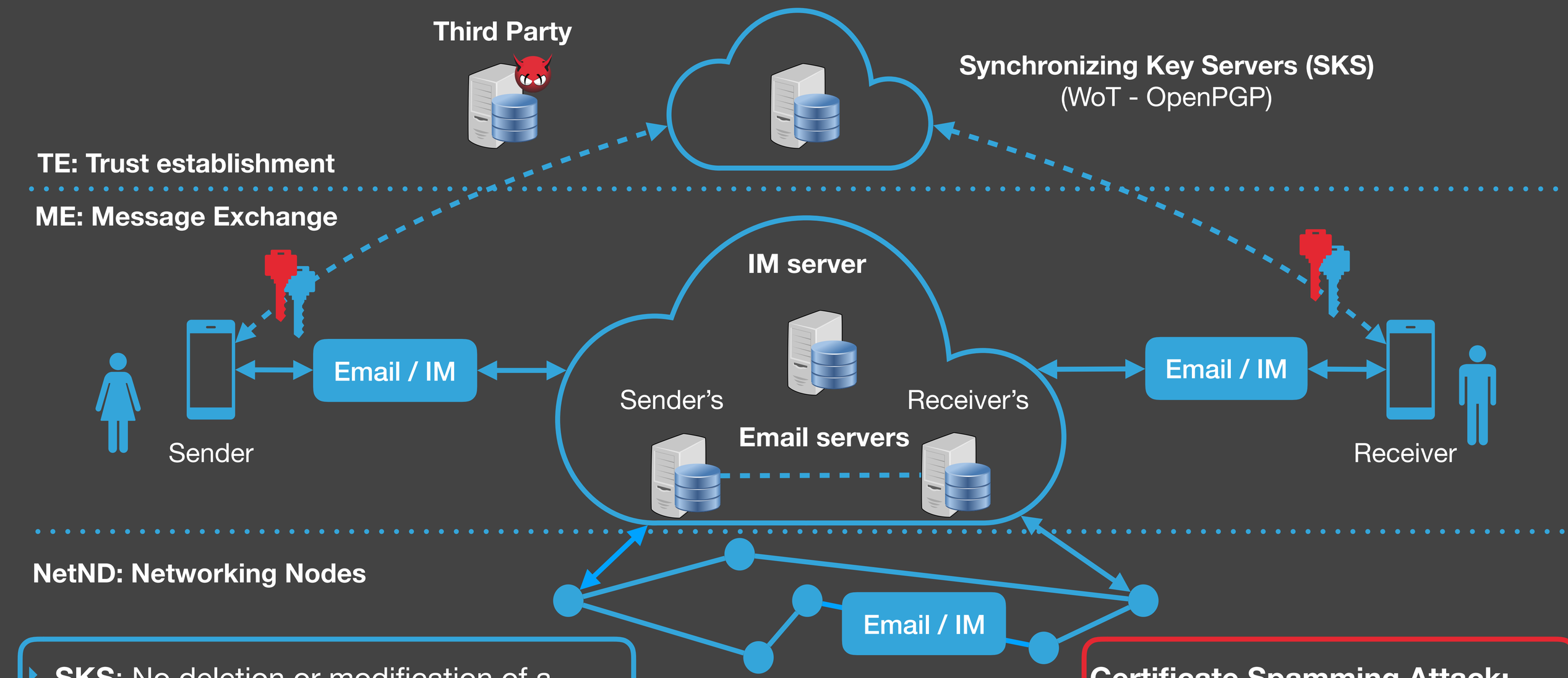
Case 2: S/MiME and Pk spoofing



S/MiME: End-to-end
- confidentiality, entity + data authentication, non-repudiation of origin

- Key managements servers: active adversaries (MiTM - no confidentiality)

Case 2: Certificate poisoning and DoS

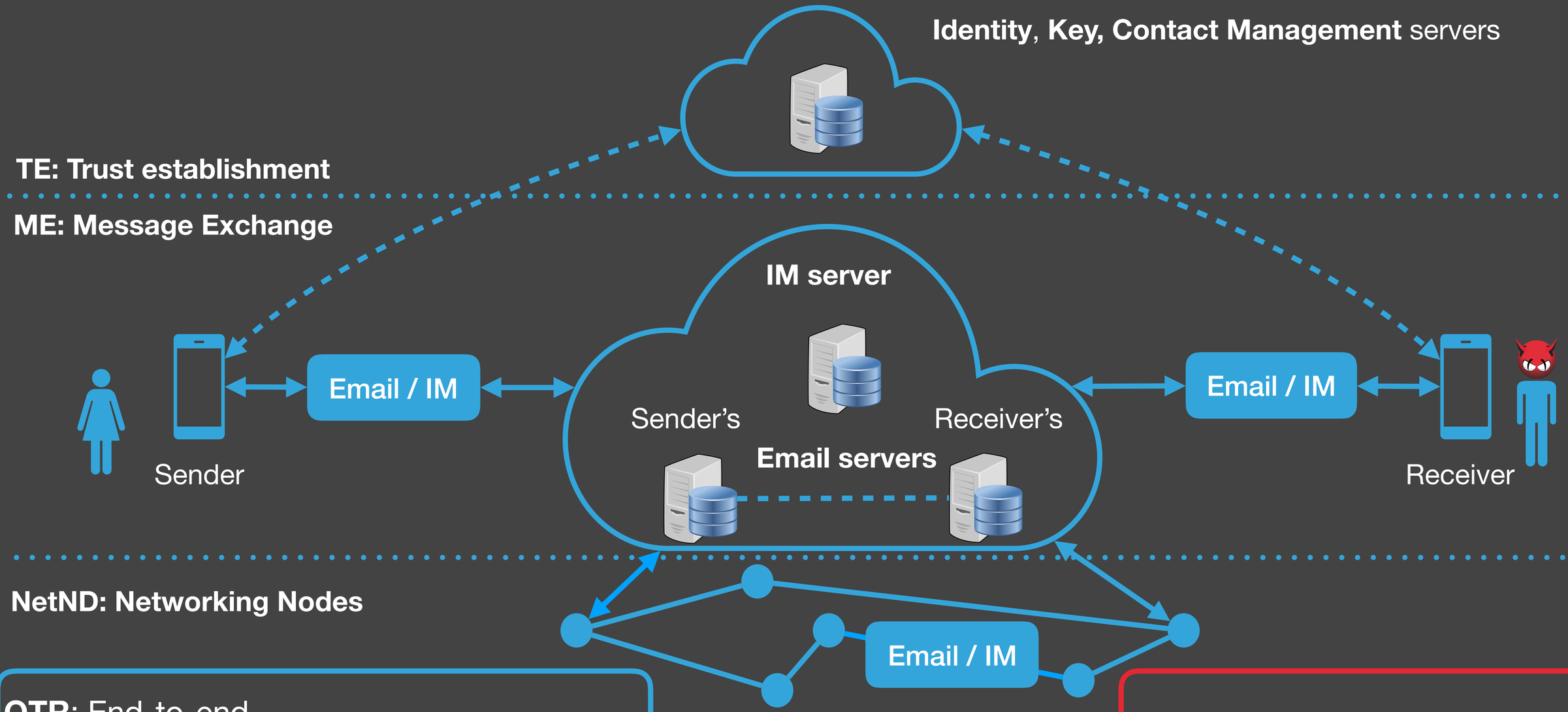


- **SKS**: No deletion or modification of a certificate (censorship resistant)
- **OpenPGP**: WoT - self signing certificates

Certificate Spamming Attack:

- Flooding a cert with bogus sign
- ~150k sign/cert ~45Mb/cert

Case 1: Non-repudation and plausible-deniability



OTR: End-to-end

- confidentiality, entity + data authentication, forward secrecy, deniability

- Requirements can be conflicting

PRIVATE EMAILING AND INSTANT MESSAGING

FUTURE DIRECTIONS?

Future directions: other issues that can affect private messaging

Why Johnny Can't Encrypt:
A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar[1]
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

USENIX'99

Why Johnny Still Can't Encrypt:
Evaluating the Usability of Email Encryption Software

Steve Sheng
Engineering and Public Policy
Carnegie Mellon University
shengx@cmu.edu

Levi Broderick
Electrical and Computer Engineering
Carnegie Mellon University
lpb@ece.cmu.edu

Colleen Alison Koranda
HCI Institute
Carnegie Mellon University
ckoranda@andrew.cmu.edu

Jeremy J. Hyland
Heinz School of Public Policy and Management
Carnegie Mellon University
jhyland@andrew.cmu.edu

arXiv:1510.08555'16

Why Johnny Still, Still Can't Encrypt:
Evaluating the Usability of a Modern PGP Client

Scott Ruoti, Jeff Andersen, Daniel Zappala, Kent Seamons
Brigham Young University
{ruoti, andersen} @ isrl.byu.edu, {zappala, seamons} @ cs.byu.edu

SOUPS'06

- Usability issues:
  - Key management (e.g., Openpgp)

User threats: backdoors

US, UK and Australia urge Facebook to create backdoor access to encrypted messages

Julia Carrie Wong • Last modified on Fri 4 Oct 2019 02.51 BST

This article is more than **1 month old**

Facebook says it opposes calls for backdoors that would 'undermine the privacy and security of people everywhere'

Credits: www.theguardian.com

Australia's Encryption-Busting Law Could Impact Global Privacy

Australia has passed a law that would require companies to weaken their encryption, a move that could reverberate globally.

Lily Hay Newman • 12.07.2018 12:45 PM

Credits: www.wired.com

Backdoors for wiretapping communications

Digital privacy of correspondence

Future directions: post-quantum key exchange for private messaging

Post-quantum cryptography a major challenge, says expert

November 9, 2018

Post-quantum cryptography will be a major challenge for the next decade at least, accord of cryptography at KU Leuven University in Belgium.

Chevy and Ford are losing market share by ditching small cars, report says

Bart Preneel:

- "10 years to switch to quantum resistant cryptography
- Data needs to be kept confidential for 10 to 50 years,
- Organizations should start planning to switch now”


That's all Folks!

QUESTIONS?

Credits: KU Leuven

iraklis.symeonidis@uni.lu