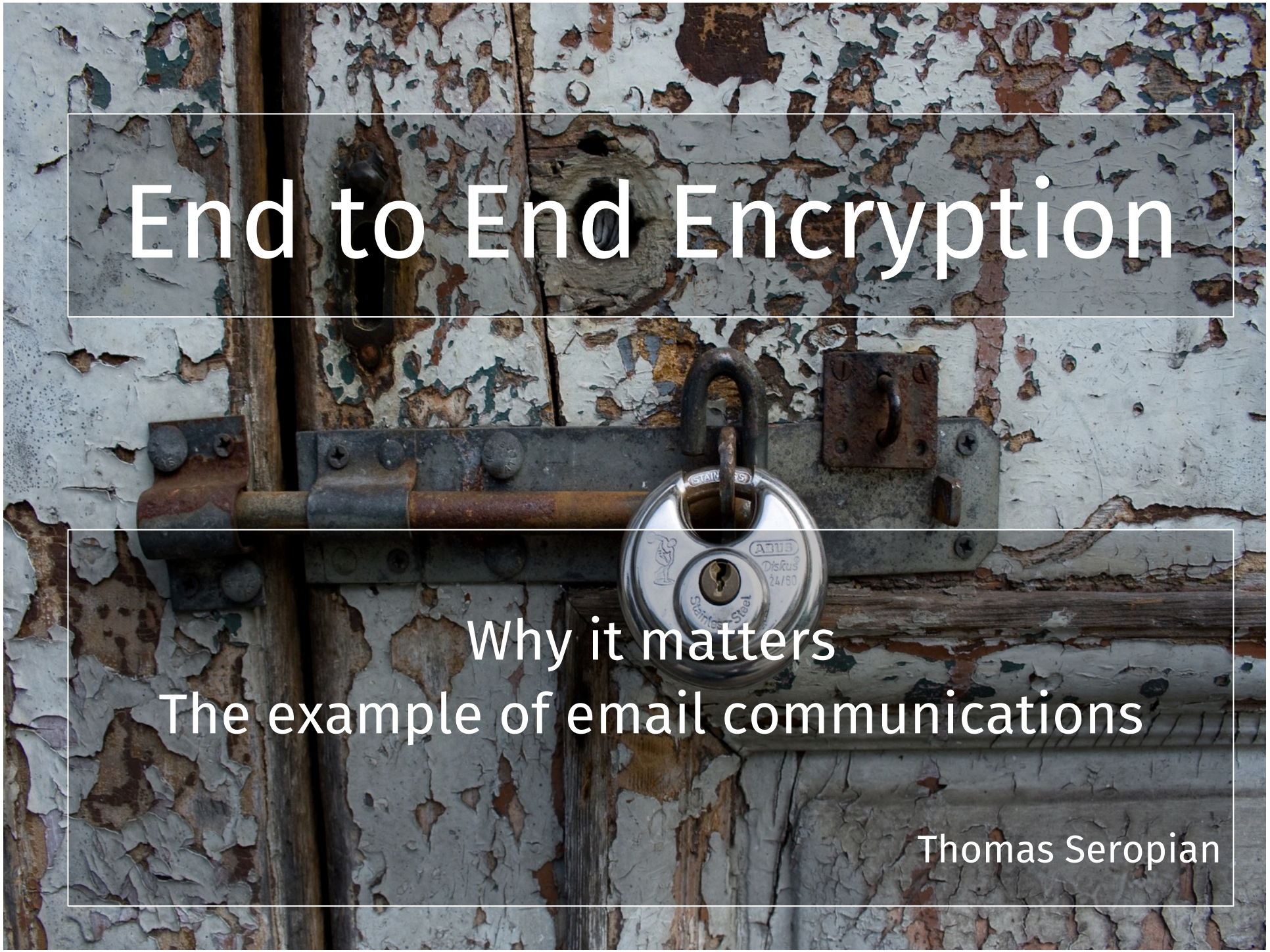
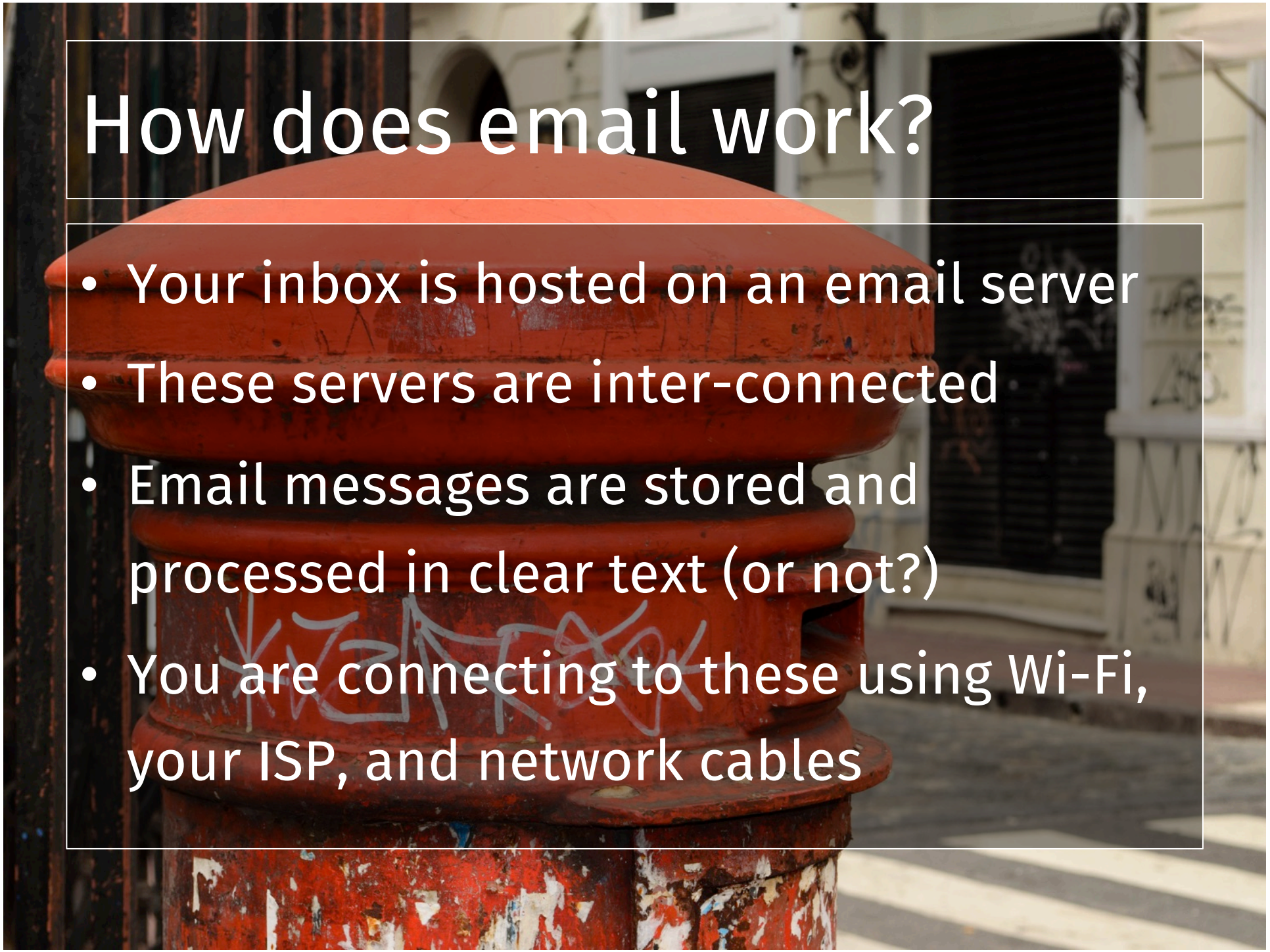


End to End Encryption

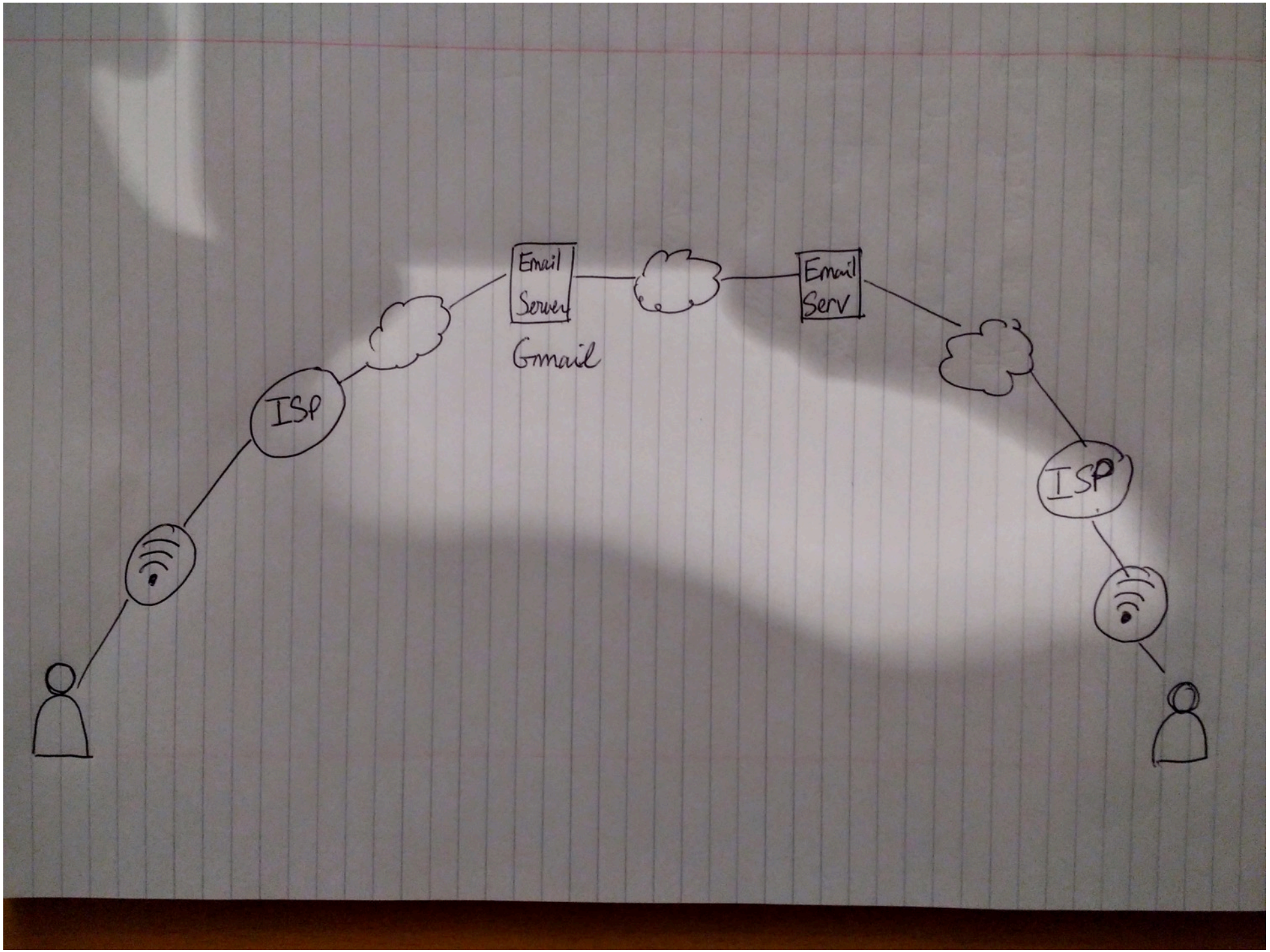
Why it matters
The example of email communications

Thomas Seropian



How does email work?

- Your inbox is hosted on an email server
- These servers are inter-connected
- Email messages are stored and processed in clear text (or not?)
- You are connecting to these using Wi-Fi, your ISP, and network cables

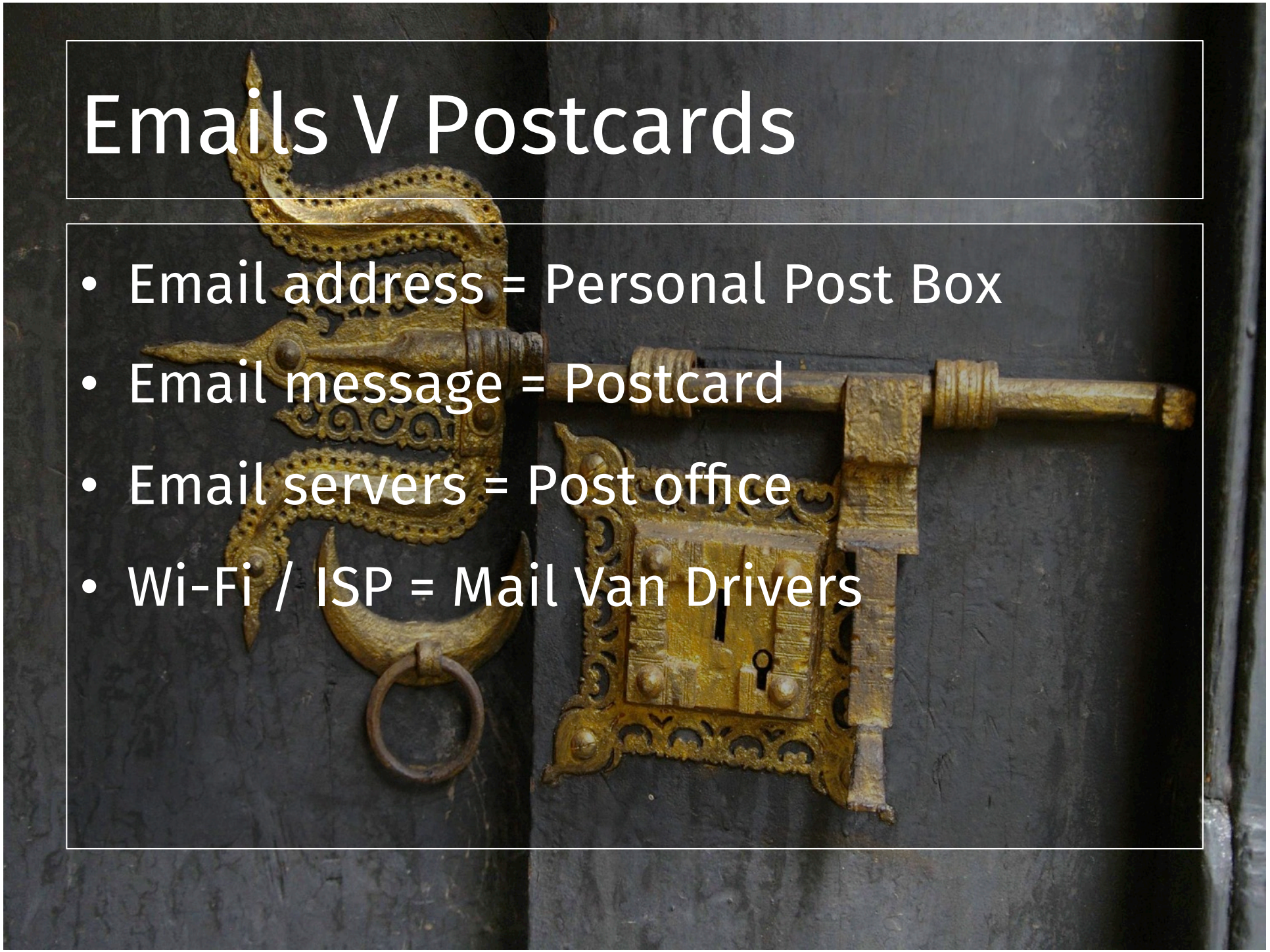

Email
Server
Gmail
Email
Serv
ISP
ISP

The internet is not a safe place

- Lots of computers connected together
- Using protocols designed in the 70s, by scientists and military
- Expected to be used by max 1000 users
- No security implemented by design
- Imagine 100 people gatecrashing a house party with no locks on the doors!

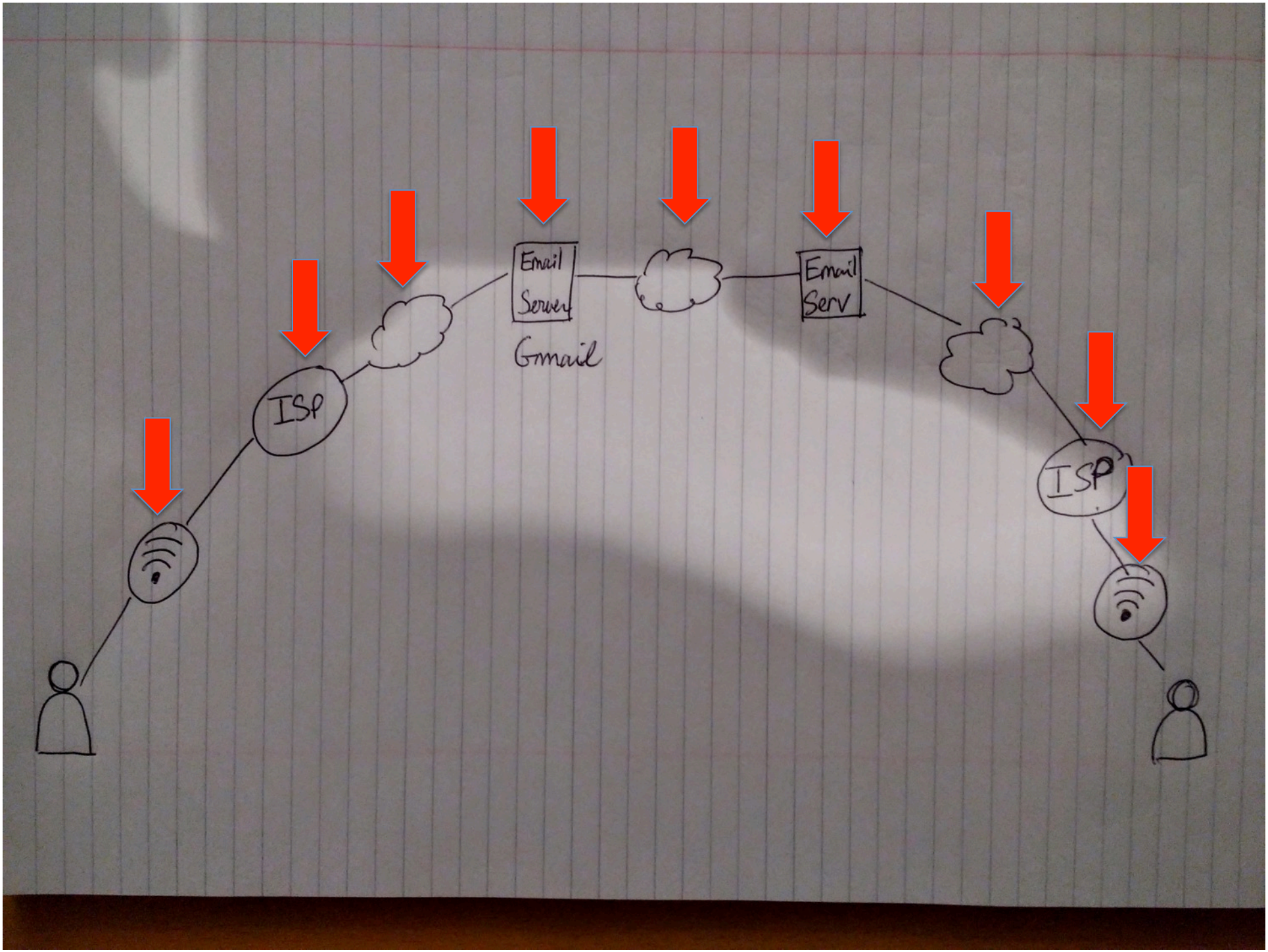
You are receiving a postcard

- Can your mailman read your postcards?
- Can the van driver read your postcards?
- Can your neighbours access your PO box?
- Can they ask your landlord for a key, forge one?
- Can they give it to a private detective?
- Is the sender the person they claim to be?



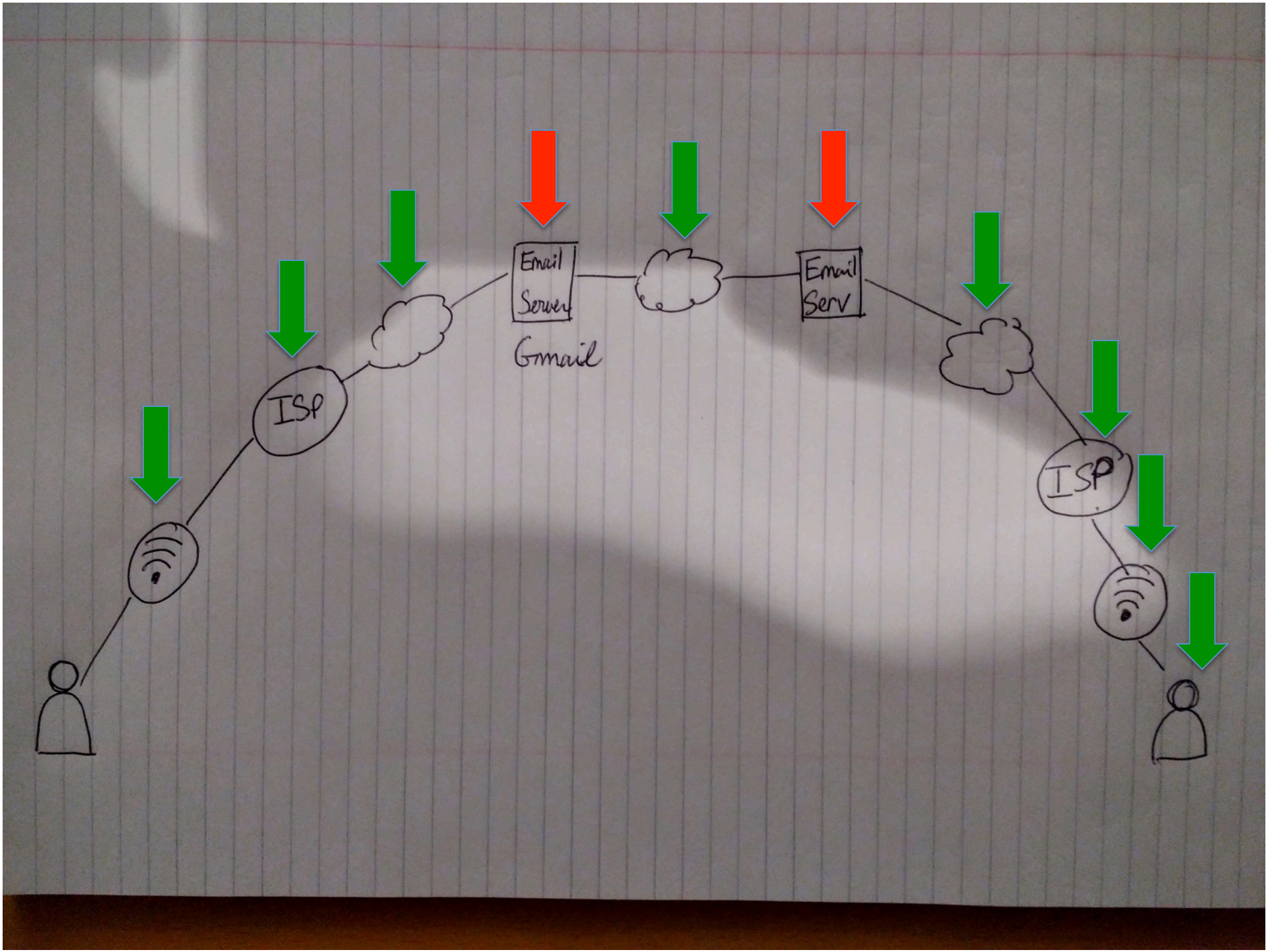
Emails V Postcards

- Email address = Personal Post Box
- Email message = Postcard
- Email servers = Post office
- Wi-Fi / ISP = Mail Van Drivers


Email
Server
Gmail
Email
Serv
ISP
ISP

Transport Layer Security

- Communication security over a network
- Encrypting communications on a network (previously called SSL)
- The van driver cannot access the content in the mail bag (but your mailman can)
- Gmail & Facebook provide TLS (HTTPS) however …

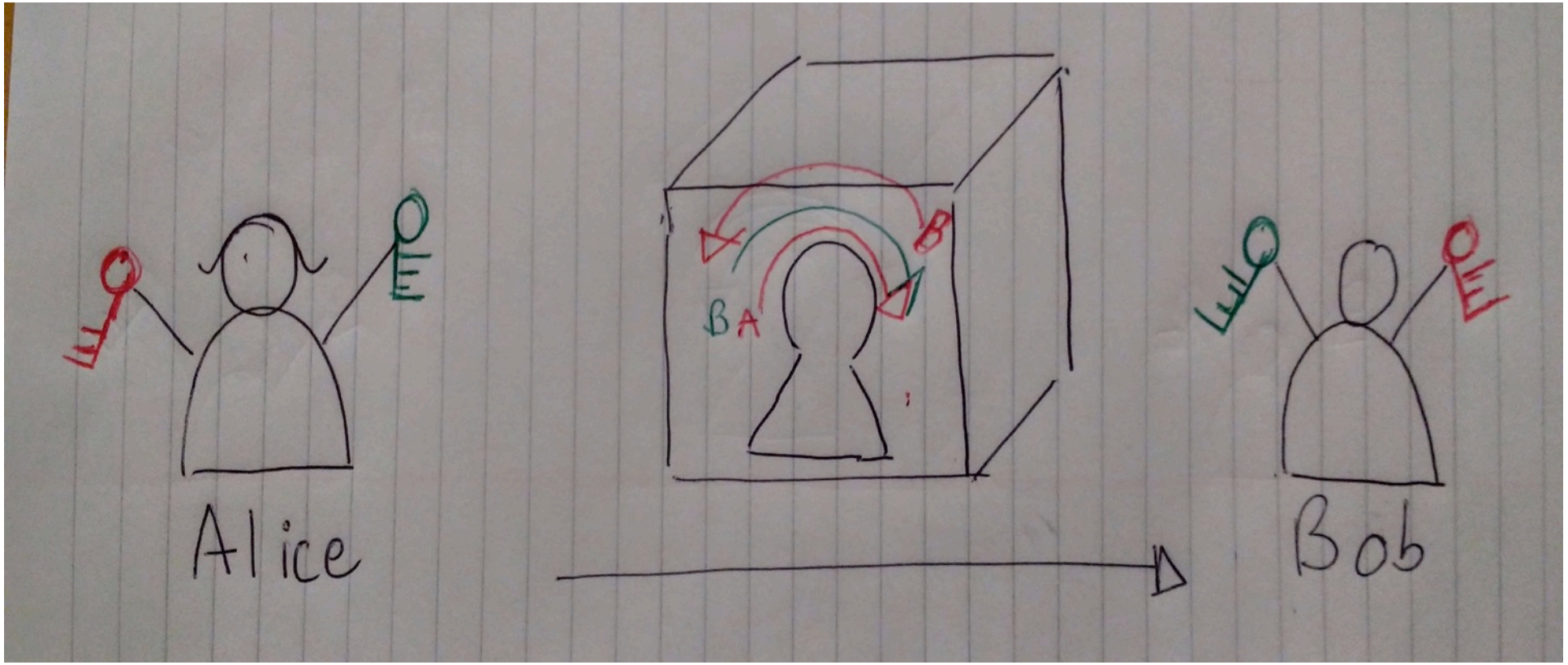

Email
Server
Gmail
Email
Serv
ISP
ISP

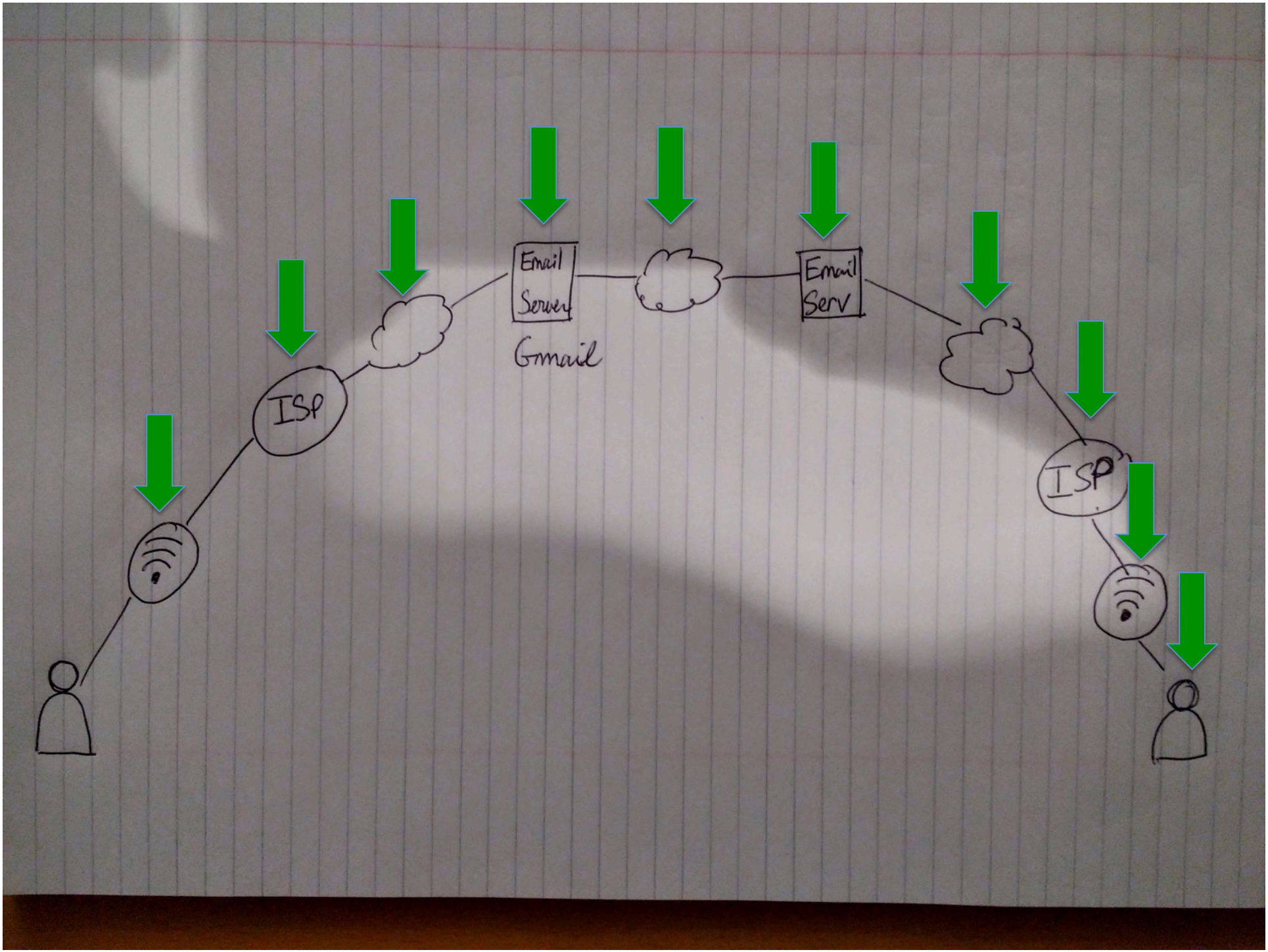
End-to-End Encryption

- Put your postcard in a safe and send the safe via email
- Each safe has a special lock that only you and your recipient can trigger
- You need to exchange keys in order to send messages to each other
- Anyone without the key is unable to open it

Each user has a pair of keys.

- Public Key : to be shared with recipients
- Private Key : to be kept in a safe place. No one else has access to it




Email
Server
Gmail
Email
Serv
ISP
ISP

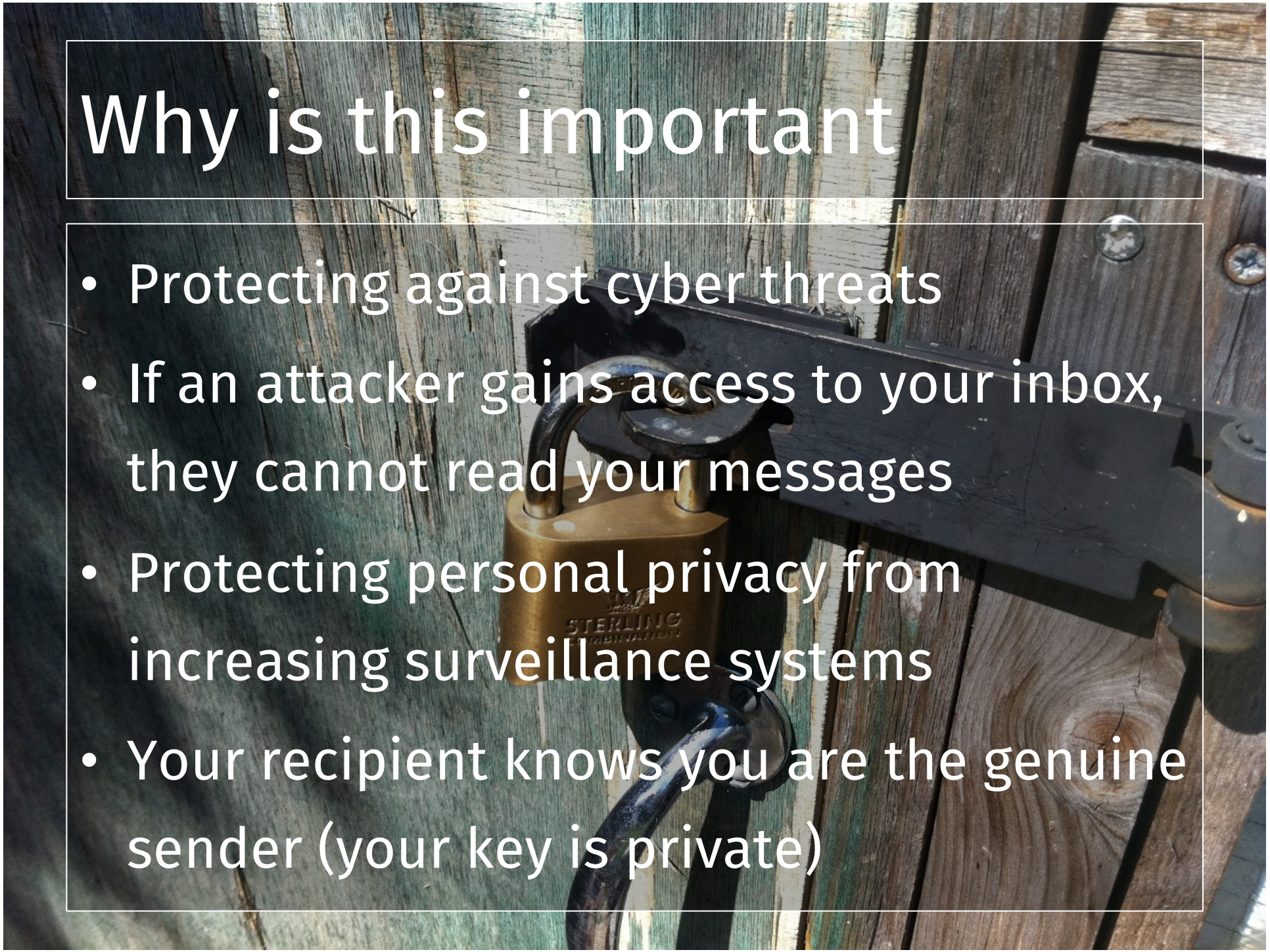
Thomas Seropian <thomas@seropian.io>

Fri 03/06/2016 21:26

To: Thomas Seropian

-----BEGIN PGP MESSAGE-----
Charset: utf-8

hQIMAycQPWD9PkCCAQ/+LFOJYdS7Jfb1S3tCDvB/N8K5z7DJ1lhVEAKQn5eSd+xF
newpRzoQfVFgMmjv+G6kKrnsHyEvJGKD3/oYimH2wCxlArMTCN475EU2fMlVgOsr
E+laUrypLE5wwaT9T0OmJNFmvSGa8eub36vH2988nlM9GMjKBMTl8WLiTy3bfXzw
NRiekBkFbe05dJ/HRNhmibxyl028R6zBoFQndH1DPM8VxwgBHqziLFmrbt/5PwVz
QduN7qBaxoWFOPP04nAFoP3z6Sfi+zYxACHVYZdKkj4u4iQAuwLdjIr0+rXuDa/k
ytXs/jw1pm21wKPZ4F2VgZXy1/m4fxgyjBcbHP8mgMsTxJuALp11tKhDdg9cvQAG
OysWJgAZsJxK99aZGiGKnntP7WsshcQazgIUawBUDMzee88p7zyeiFudInwgQj/V
m1kdEe0tEuhkRmQB0ayQUW9Mr8PGe1F2k2q+hJKVg3JISZmN0jL7wf5hJFce0afs
Bz2v+XPihN+Ernwen5arlbyB5egnnNYy6S6vNPfBZLd6654WuN9YccYRX7wl9GbZ
Nn1zCz6d/EOQsML2YJuRbLnNRCQMFSmxIDfrCKLS2ztvXNw7Gf+5CnqD1PM/8Yn/
xCTqB5M2UCTICYWDoI3UTkCV8lfZipuW91uux1kU0Mtt3IJ8dHdlw4U4t7vEFLmF
AQwD/f641hNdQbQBB/9+VCvVpy786fX4sSQdVrBOT8A2pOzOe9WfiNjU3H3oSuC3
iHjkAJF6GSHAoBzVAQKwE6tRfxHn8wo3nHrFTTYWV3/26Uj83sAh4Ccmo5k6dR0L
amMi7i7GQcyoL42QMYp+ccfyIgXfn1RT8MWmDtVs0rRMZXf0tMJL4l6vltlINeXv
qNmaeV7a3ugsZ3cTHOQK4bEsn7KgXiNHN7rs4Uw+/spI1P7JdWPlYPF0D9FSr/f2
eh9gelsL3cmRRrN3uYENMGc+DKVSxwwv7SD996XB2xutnuzUhup9Q/OpwgEOwujU
RghQE5I4OMdP8Cm69BlC/2ErBSgWhOt9VqnHKD190n0B6asqxINz4bwGtE9kPChV
rbm9UmuhWVHU6PaVhfxfTdOYCKcS3EZ9aQZKAQMcpBzjdMz0V7xaEf6OWRux2ScW
rtWL30wp0vdapTzkGe9Fk/a0nSn1scLJfFh81inmlN9XzmELEbfBpbUz7clxHHMU
vnlpbl/K0rhpPLid9Q==
=zUWT
-----END PGP MESSAGE-----



Why is this important

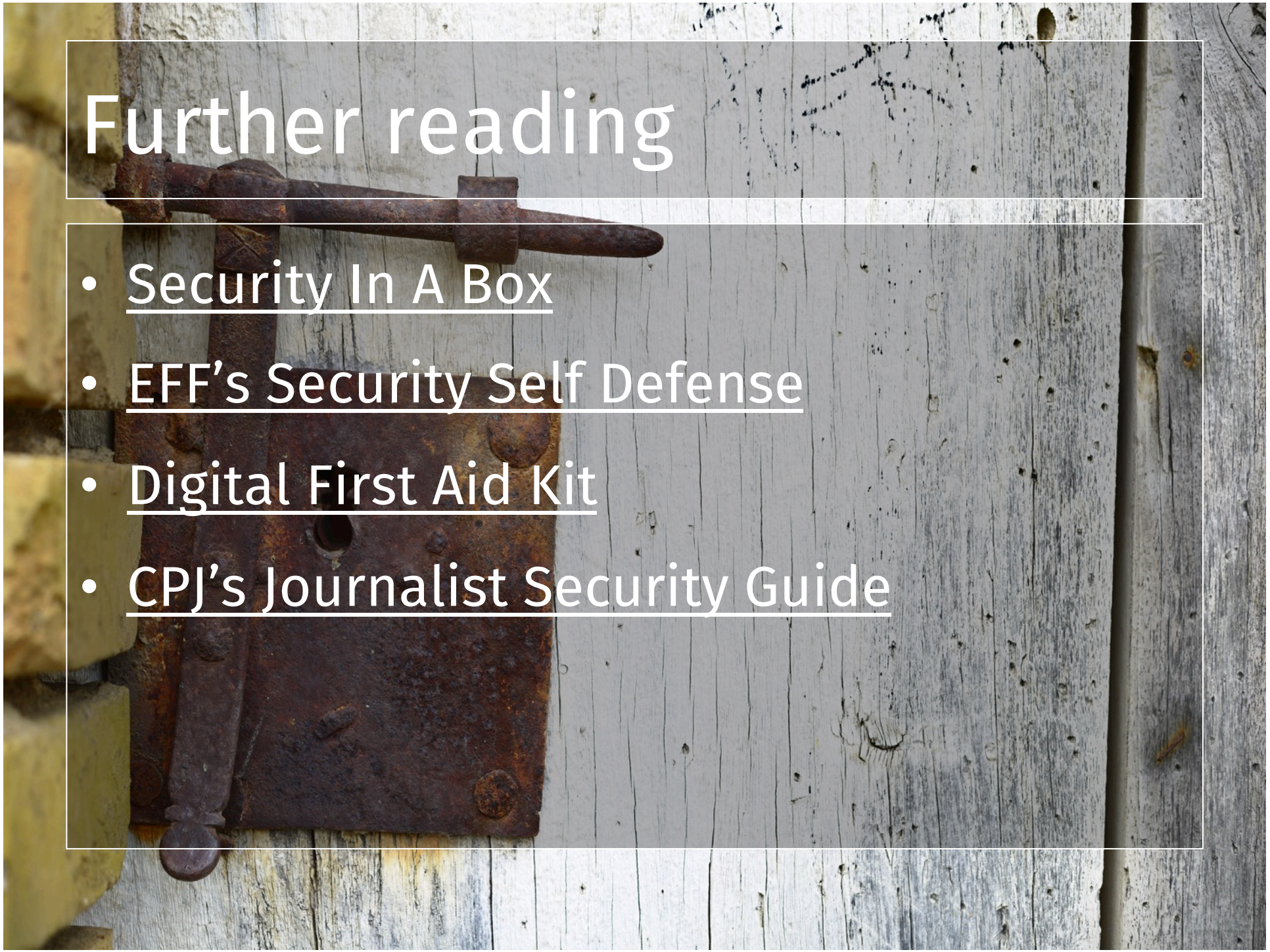
- Protecting against cyber threats
- If an attacker gains access to your inbox, they cannot read your messages
- Protecting personal privacy from increasing surveillance systems
- Your recipient knows you are the genuine sender (your key is private)

E2EE in the news

- Whatsapp rolling out E2E encryption for 1 billion users
- Snowden was using PGP to communicate with Laura Poitras and The Guardian

Thank you for your time

- Questions, comments?
- Contact me
  - thomas@seropian.io
  - PGP Key : 0xfc944ab6
- Slides
  - http://seropian.io/assets/files/e2ee.pdf



Further reading

- Security In A Box
- EFF’s Security Self Defense
- Digital First Aid Kit
- CPJ’s Journalist Security Guide