The state of email in 2015

Martijn Grooten, Virus Bulletin

TROOPERS15, 19 March 2015

Me, myself and I

TROOPERS

virus BULLETIN

Anna sends an email to Bob

TROOPERS

virus BULLETIN

Anna sends an email to Bob

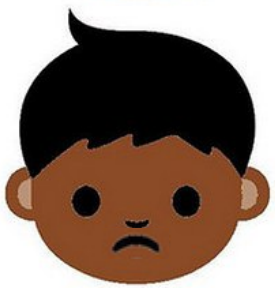
Anna can send emails very easy and very fast.

She can do so without needing Bob's permission.

Spam is a feature of email, not a bug.

It’s the 1990s and here’s Spike

“Hi, bob@hismail.com.
Do you want to buy a
fabulous [illegible] offer?”

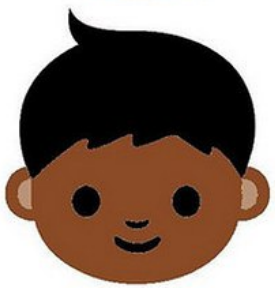


TROOPERS

virus BULLETIN

Early spam filters: content based

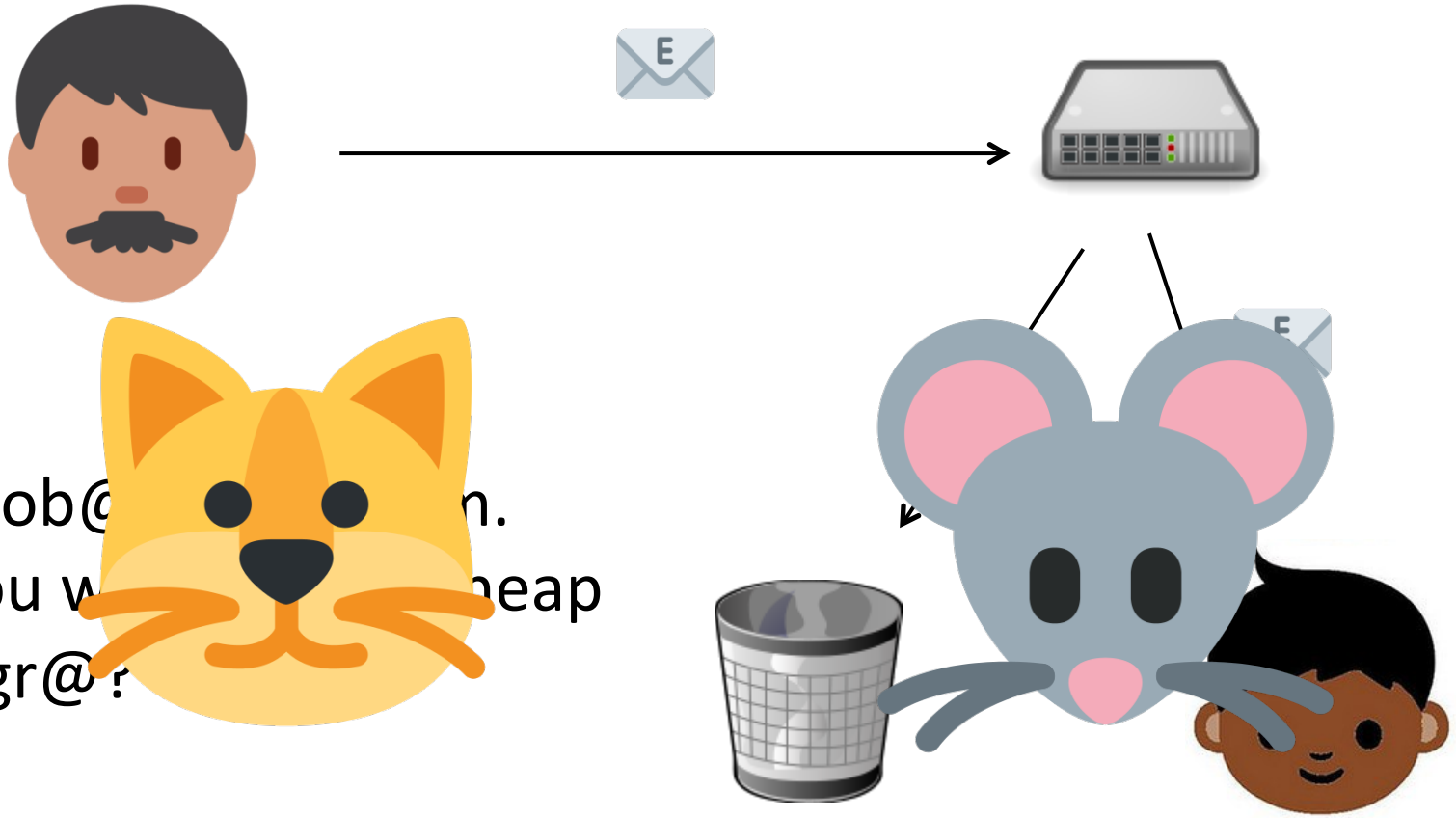
```
if $email contains “VIAGRA”
then
      send to trash
else
      send to Bob
fi
```



TROOPERS

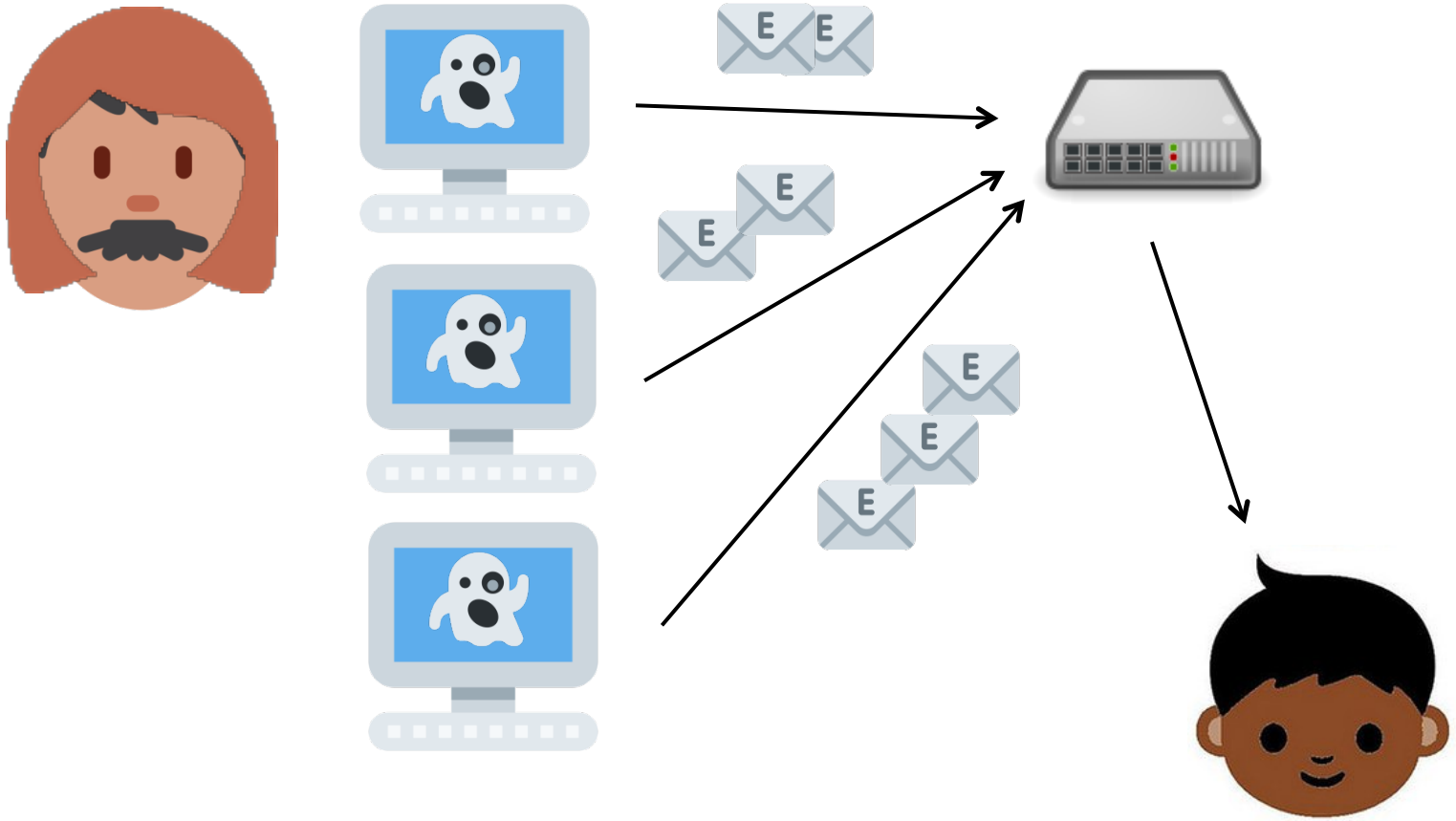
virus BULLETIN

Spike thinks he’s cleverer than that



“Hi, bob@ n.
Do you w eap
V1@gr@?

Spike started using hacked computers



…and pretending to be Anna

TROOPERS

virus BULLETIN

Hold on. Isn’t email totally broken!?

After all, anyone can rent a botnet to bombard Bob with emails claiming to come from Anna. Email does not have a built in mechanism for Bob to verify the source.

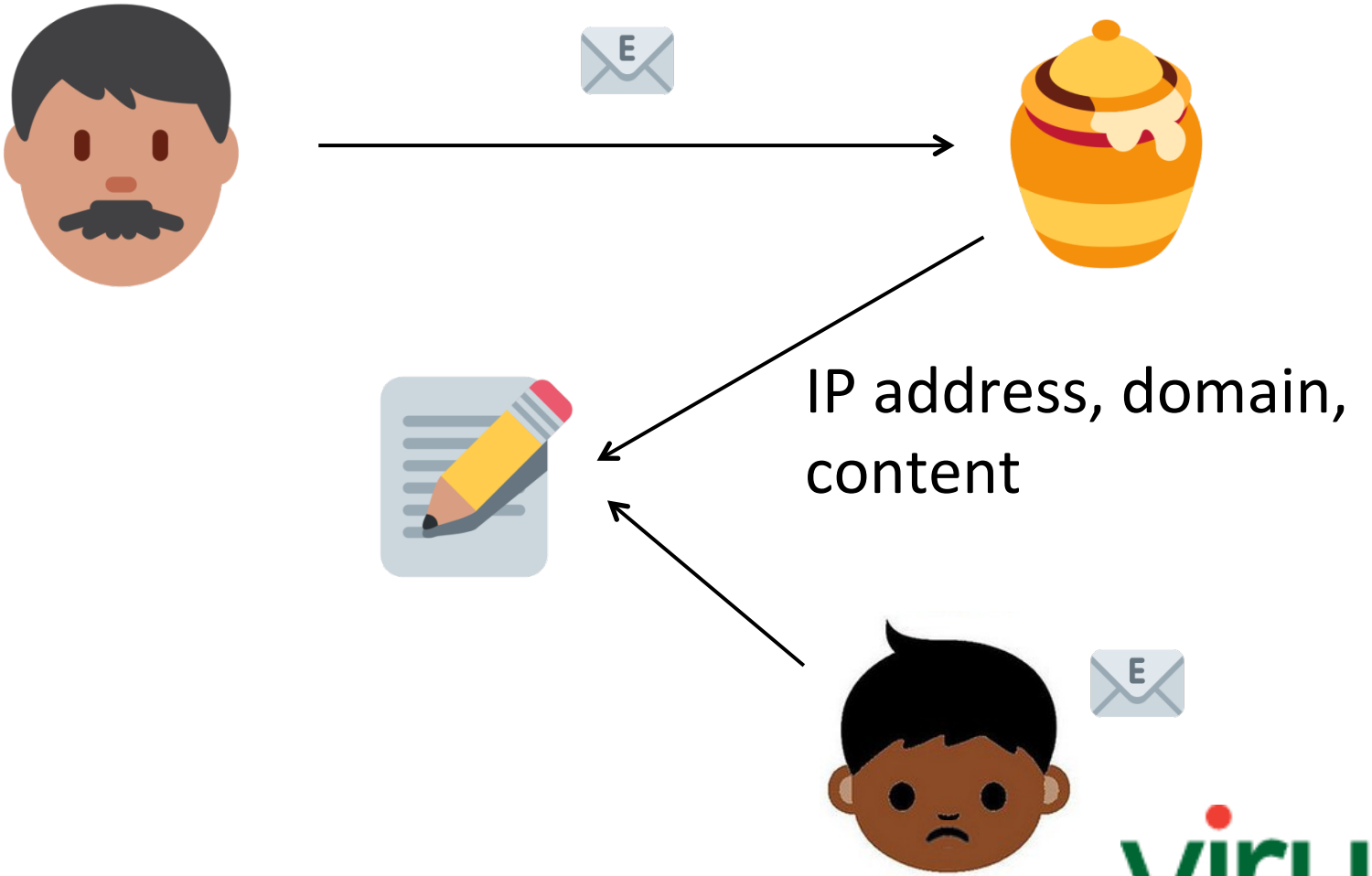
10 years ago, some pessimists thought that email was going to die soon.

Except we are cleverer than that.

Mitigating the spam problem

- Content-based filters
- IP- and domain based blacklists
- Outbound filters
- Botnet takedowns
- Anti-spam legislation
- SPF
- DKIM
- DMARC

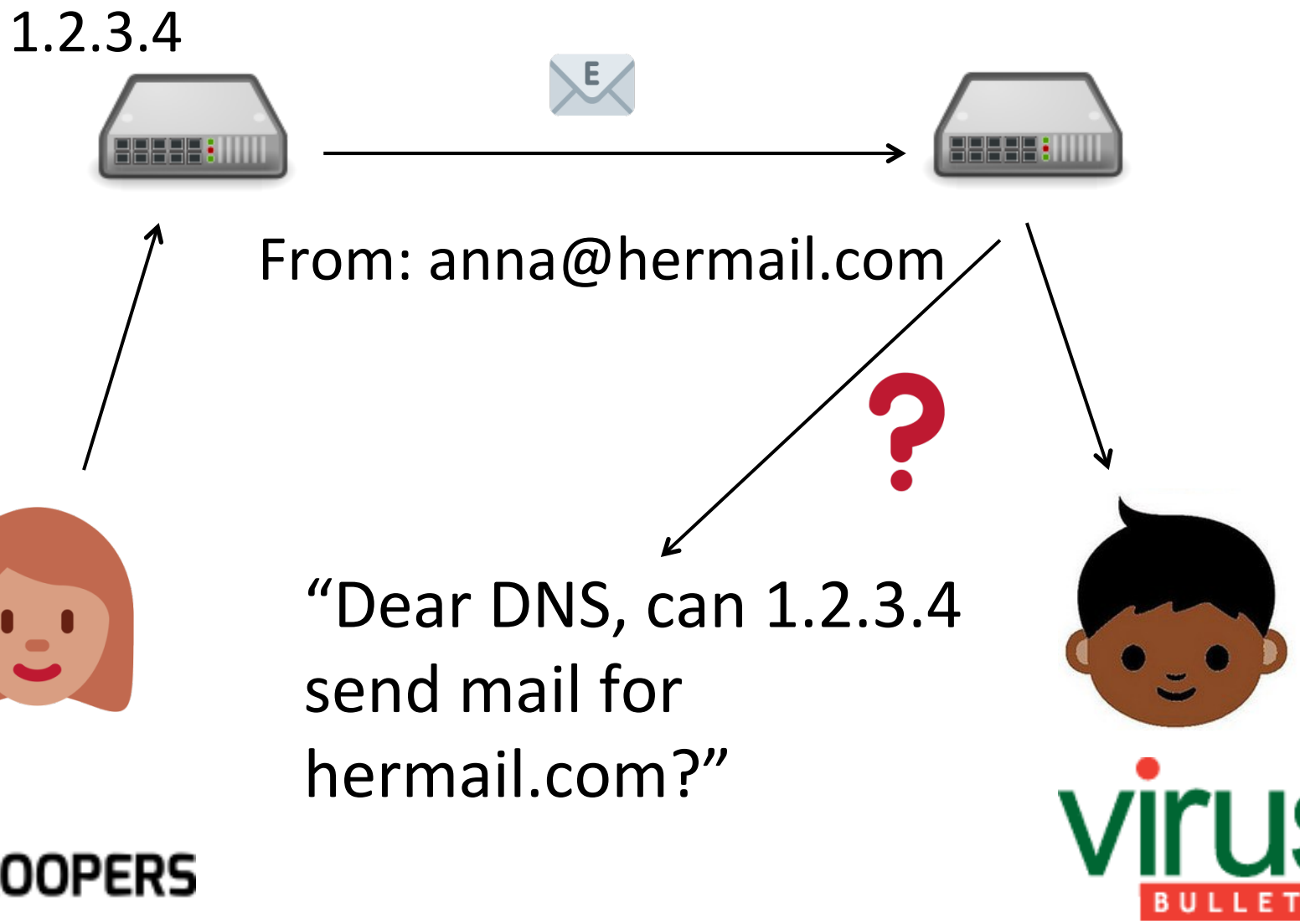
Filters and blacklists



TROOPERS

virus BULLETIN

SPF



TROOPERS

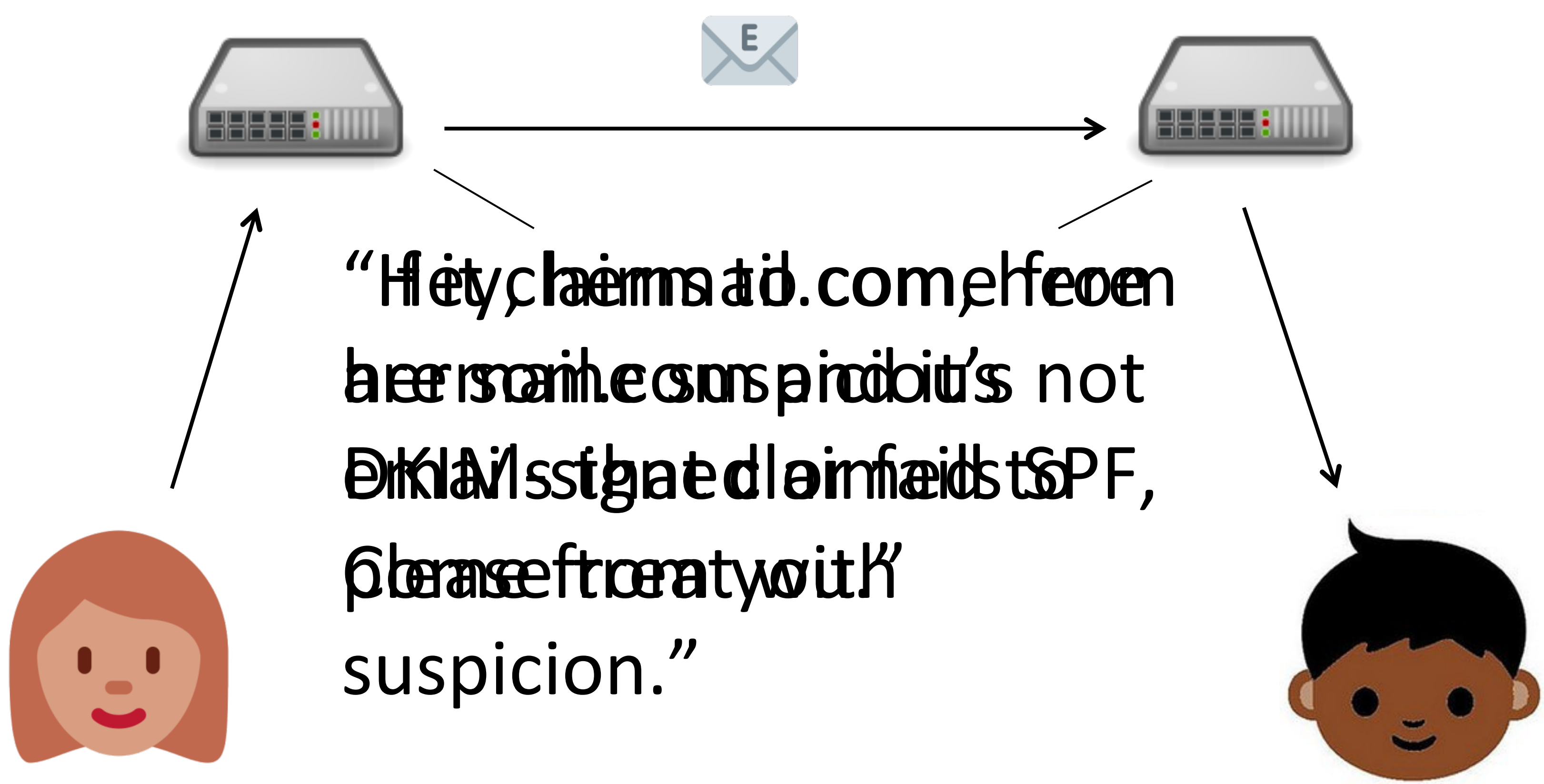
virus BULLETIN

DKIM

TROOPERS

virus BULLETIN

DMARC


“If it claims to come from hermail.com and it’s not DKIM-signed or fails SPF, please treat with suspicion.”
“Hey, hermail.com here, are some suspicious emails that claim to come from you.”

The State of spam in 2015

Spam remains a problem in 2015, but it is fairly well mitigated. Bruce Schneier called it a rare success story in cybercrime.

TROOPERS

virus BULLETIN

Oh noes! IPv6 is coming

TROOPERS

virus BULLETIN

Good news and bad news

Email (SMTP) takes place in the application layer, IPv6 in the network layer.

Spam filtering makes heavy use of the IP(v4) address.

More good news and more bad news

We don’t need all that many mail servers. They can just stay on IPv4.

The IPv6 momentum can’t be stopped. Not even for mail servers.

Solutions?

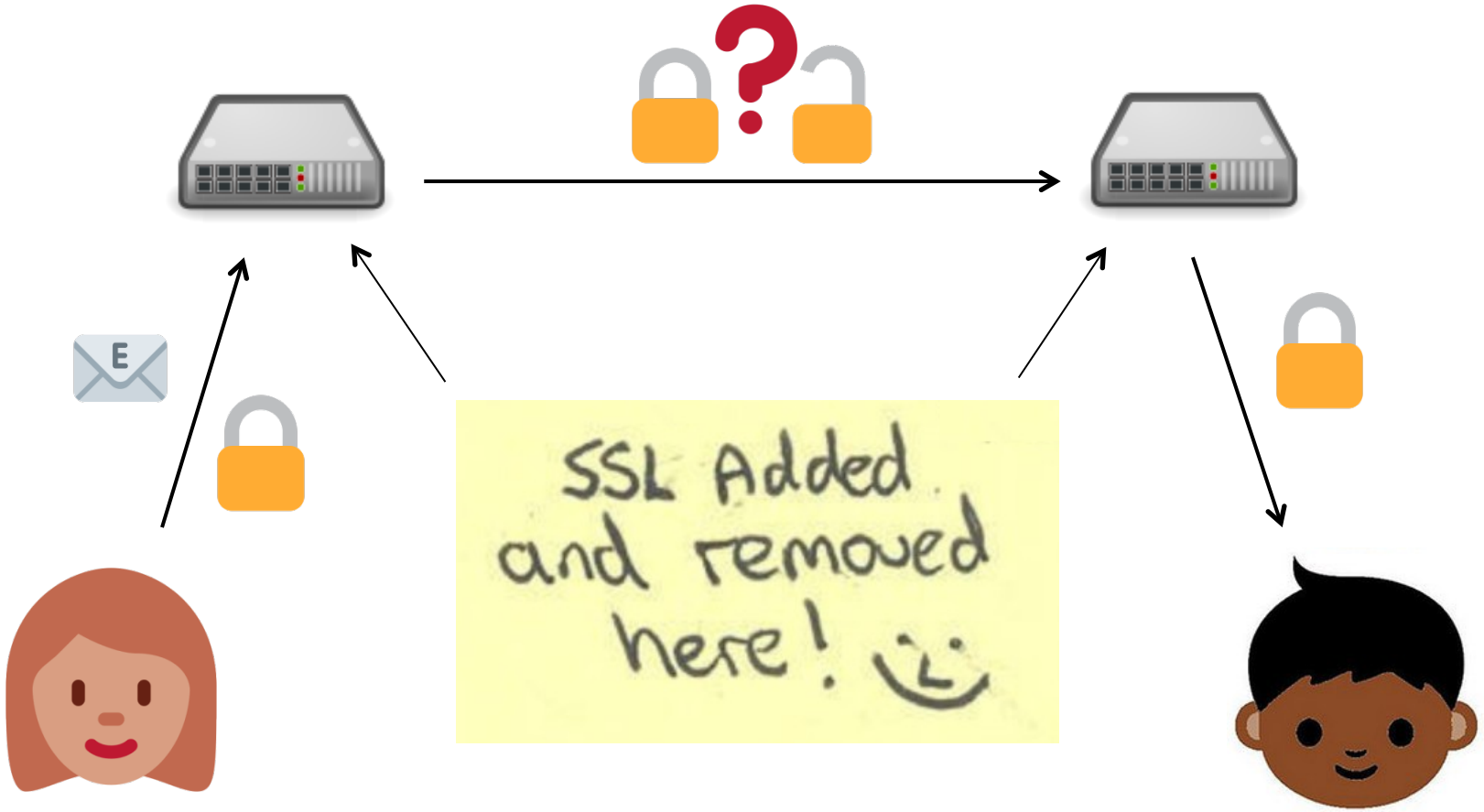
Make our blacklists adapt to IPv6:

```
2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.2.1.0.c.b.a.0.8.b.d.0.1.0.0.2.zen.spamhaus.org
```

And hope people will follow The Rules.

Ditch IP addresses; use domain names instead (DKIM, SPF).

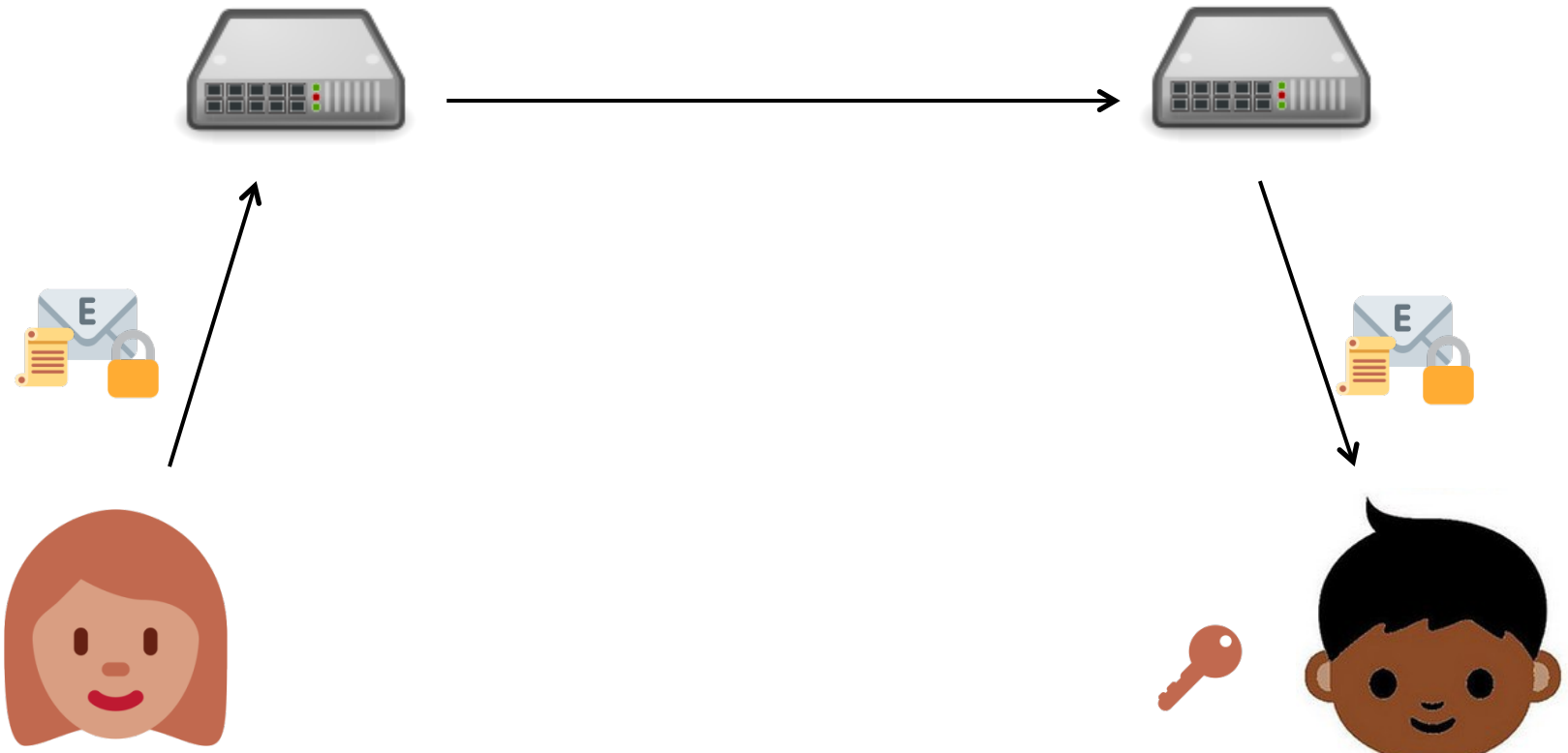
Anna and Bob, post-Snowden



TROOPERS

virus BULLETIN

PGP



TROOPERS

virus BULLETIN

What PGP means

“Anna encrypts her email using what she has been made to believe is Bob’s private key.

Bob is able to verify that the email was sent by someone in possession of what he has been made to believe is Anna’s private key.”

What we want PGP to mean

"Anna encrypts the email so that only Bob can read it. Bob can verify the email came from Anna."

This translation doesn't scale well.

And PGP leaks a lot of metadata

Of course, metadata is only metadata.
But then, it is still metadata.

It’s good to keep in mind

Targeted surveillance by intelligence agencies isn’t part of most people’s threat model (nor should it).

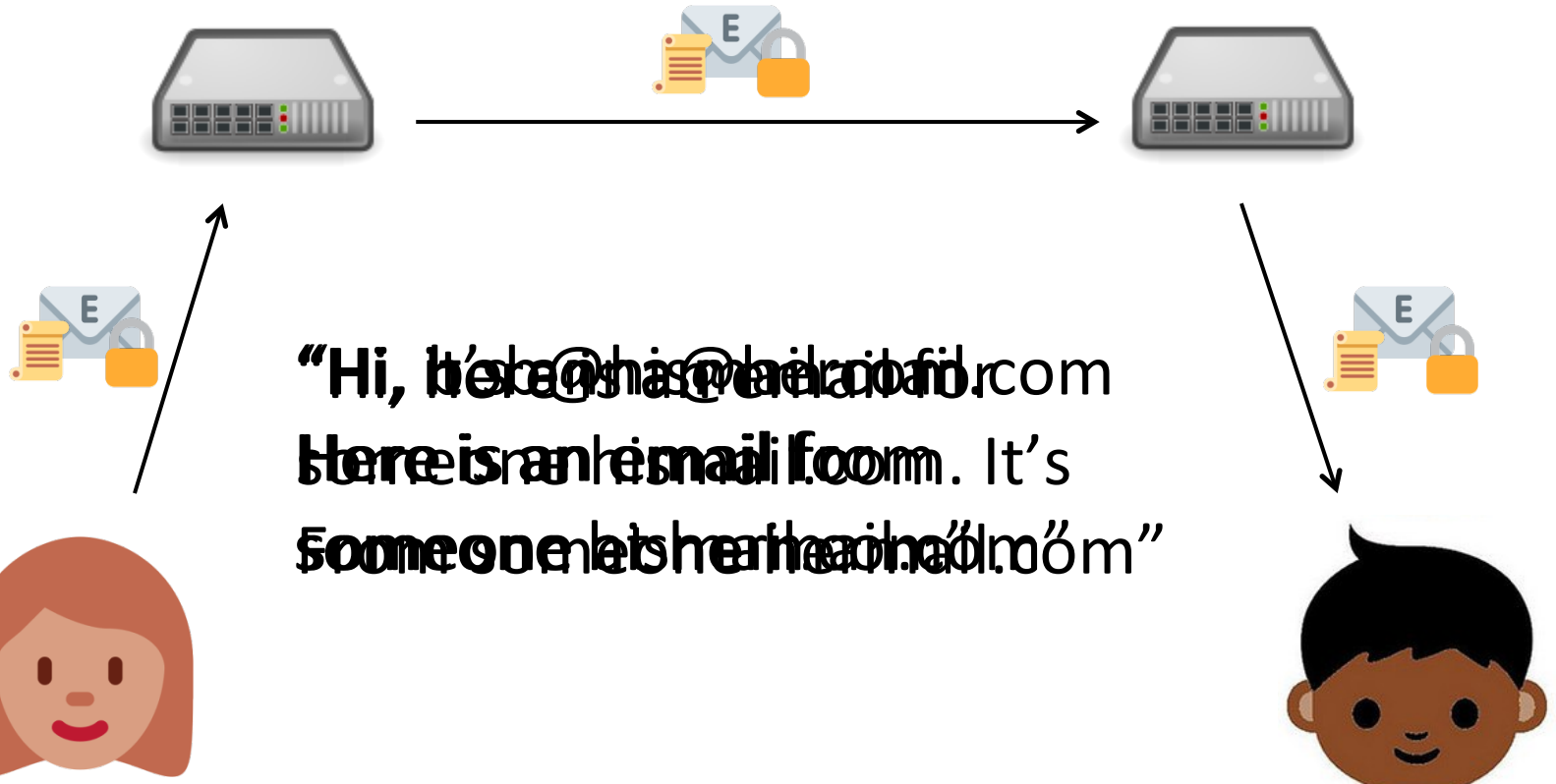
2,000,000,000 email users can’t be wrong. Or at least they won’t change habits easily.

Cryptography is hard. Don’t try it at home.

TROOPERS

virus BULLETIN

Dark Internet Mail Environment



TROOPERS

virus BULLETIN

Why I love DIME

- Written by people who understand both encryption *and* email.
- Integrates seamlessly into email; two system can exist next to each other.
- Allows users to place trust in servers (e.g. webmail).
- Users don't need to understand crypto.

But what about spam?

The 108-page DIME specification doesn't mention spam even once.

Spam filters inspect email. Do does the NSA. We can't have it both ways.

Spammers can use encryption as well as everyone else.

Why I am optimistic

We have collectively shown we're very good at fighting spam.

DIME includes various level of security and of trust. Spam filters can be integrated into these.

We can't stop spam 100% anyway.

Questions?

martijn.grooten@virusbtn.com
@martijn_grooten
www.virusbtn.com