Cool pictures and visions by oej.

Let's get serious.

1. **SECURITY:**
Always build secure platforms. Secure all communication.

2. **IPv6:**
Integrate IPv6 in every single project.

3. **OPUS:**
Give your users the audio they deserve. Use Opus.

4. **FEDERATE:**
Federate or die. Call using domains.

Let's focus.

1. **SECURITY:**
Always build secure platforms. Secure all communication.

2. **IPv6:**
Integrate IPv6 in every single project.

3. **OPUS:**
Give your users the audio they deserve. Use Opus.

4. **FEDERATE:**
Federate or die. Call using domains.

2014-02-09

#MoreCrypto and SIP

A small step to make it harder
to listen to SIP based activity.

The problem

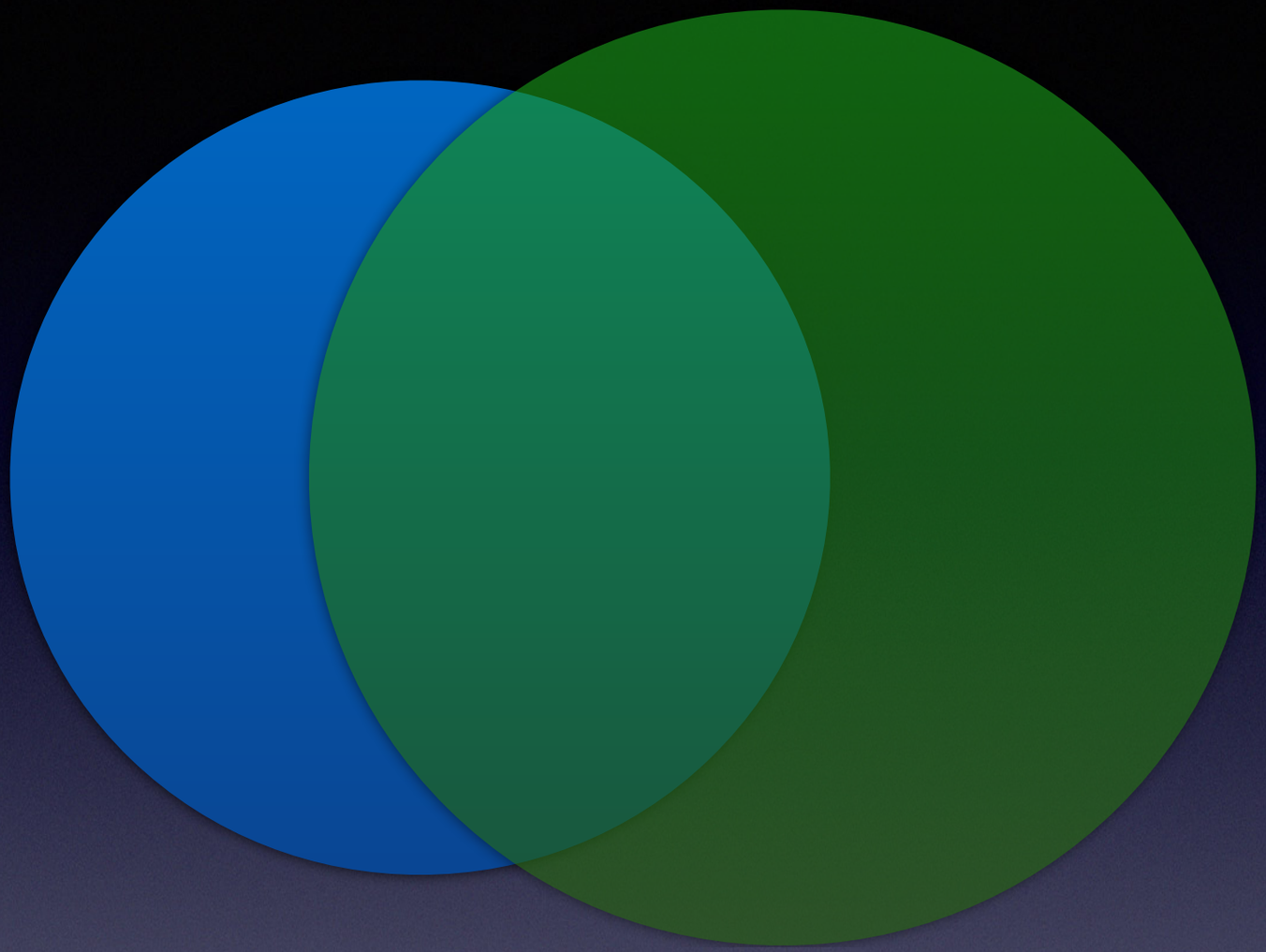
We have built an information network that is too easy to monitor. We simply trusted everyone too much in a naive way.

Sadly, we can't do that any more.

The Internet mirrors society

When the Internet was small, there was a select group of people using it. They felt is was a safe place.

#MoreCrypto

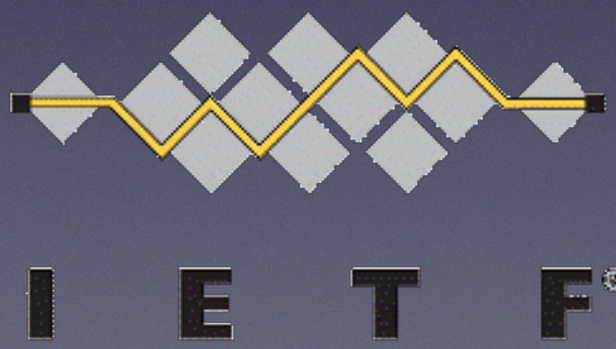


As the Internet grew and reflects more of society, we forgot to harden it. It’s time now.

#MoreCrypto

The engineers are working

The IETF is the organisation that defined most of the standards we use today to communicate.



The IETF recently decided to focus a lot of energy to add more confidentiality and security in general to the technology we use every day.

#MoreCrypto

What’s the problem?

Changing the Internet is too hard.

We are not using the security tools we have in the way they are meant to be used today.

In some cases, like e-mail and IP telephony, most of us do not use any security tools at all.

#MoreCrypto

How do we change?

The users must require change. Otherwise, very few things happen. But developers can change implementations too.

It is up to **you** and **me**.

#MoreCrypto

What needs to be done?

More crypto

Easy to use authentication

…and much more

Enhanced privacy

Stronger confidentiality

A lot of changes needs to be done in how we build services, operate them and use them.

#MoreCrypto

TLS is an important tool

TLS provides confidentiality, identity and integrity to Internet communication.

TLS is used in HTTPS:// web pages, but can also be used from applications on a computer as well as a cell phone.

TLS is based on SSL, that was a provider-specific technology. TLS is maintained by the IETF and is still being improved.

TLS

Transport Layer Security

#MoreCrypto

Start simple.

Use connection encryption wherever possible.

Use HTTPS and serve information over HTTPS

In short:
#MoreCrypto

#MoreCrypto

Why?

More crypto on the Internet **raise the cost** of listening in to our information flows, our conversations.

It does not solve all the issues, we have a lot of work ahead of us.

Using more TLS is not very complicated and can be used in most applications today.

#MoreCrypto

The work continues

Mobile apps

Web

IP Telephony

E-mail

Video Services

Cloud Services

Internet of things

The Digital home

Chat

Require #MoreCrypto!

#MoreCrypto

OPPURTUNISTIC SECURITY

Secure network traffic, regardless of what the user says.
Do whatever you can to make it harder to listen in.

Re-learning

Authenticated TLS	**Secure signalling hop by hop.**
Opportunistic encryption of sessions	***Not secure*, but harder to listen in**
SDES key exchange + SRTP	***Not secure*, but harder to listen to media**
DTLS key exchange + SRTP	**Secure if end2end**

#MoreCrypto

Opportunistic Security In SIP

Clients - UAs and Proxys - should prefer TLS over TCP and UDP.

All servers - SBC, B2BUA, PBX, Proxys should have TLS working. Certificates are available for free!

Use SRTP wherever possible.

Let's forget about the SIPS uri. It just doesn't work or help.

#MoreCrypto

Let’s make this happen.

Default to trying TLS before any other SIP transport

Always offer SRTP,
Maybe combination Rtp + SRTP

Always install TLS certificates in servers

Use SIP outbound over TLS from UAs

#MoreCrypto

A final word

"The point is not to make enforcement of the law more difficult; legal intercept is a necessary part of living in a society.

Casual retention of everyone's data, ripe for misuse, however, is not, and that's what the industry — from Google and Yahoo!, to the IETF and Tim Berners-Lee — are pushing back on."

Mark Nottingham,
chair of the IETF HTTPbis wg

#MoreCrypto

http://www.mnot.net/blog/2014/03/17/trying_out_tls_for_http_urls

More information

http://www.internetsociety.org/deploy360/tls/
https://bettercrypto.org
http://tools.ietf.org/html/draft-farrell-perpass-attack-06

#MoreCrypto