Tom Lowenthal
tom@mozilla.com
@flamsmark

mozilla

Cryptography Infrastructure

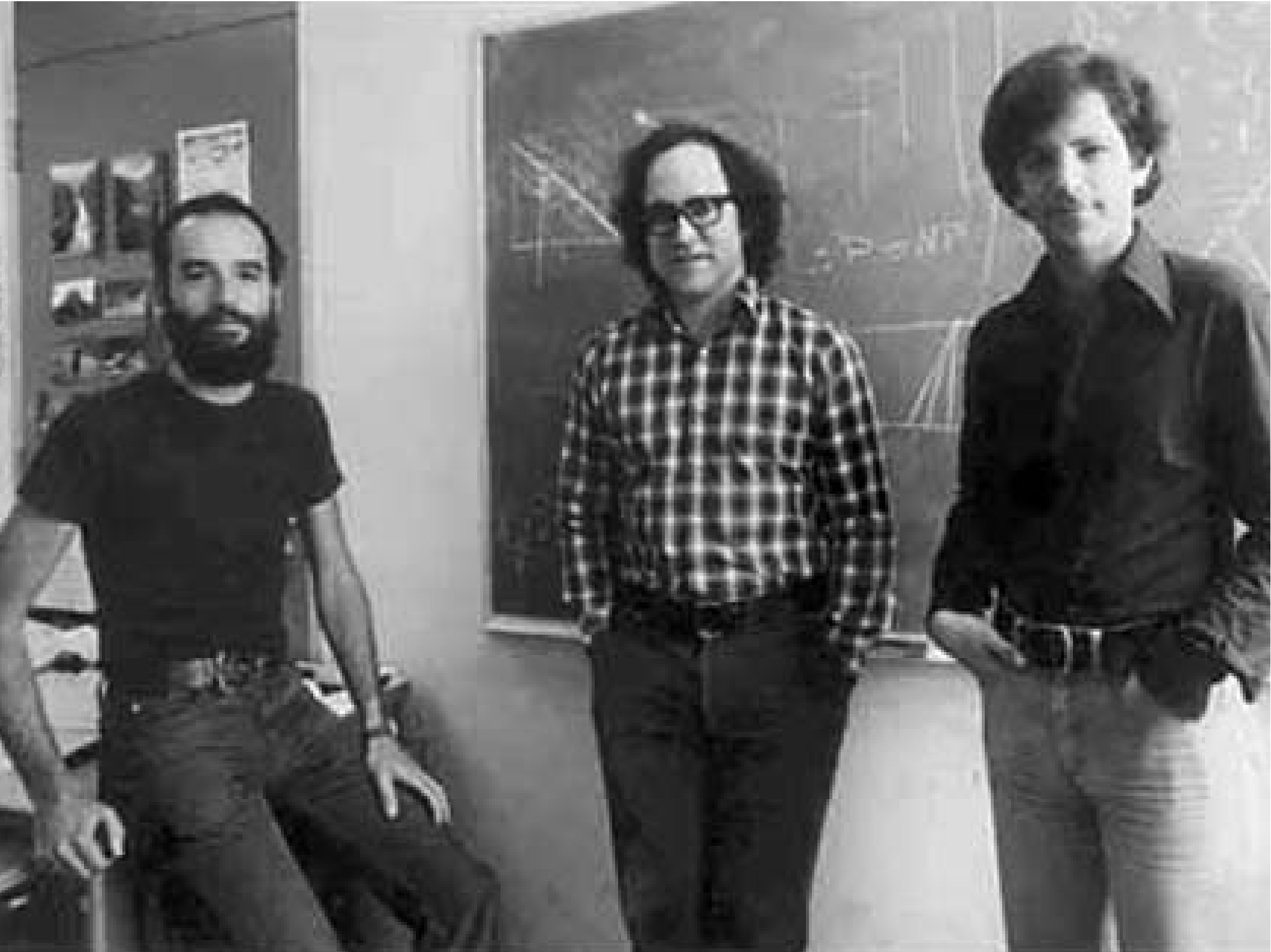
IETF 83, 2012

A fairytale origin story

Everything is beautiful and broken

Implementation details matter

Once upon a time...




TOP SECRET

the magic of RSA:

Public key cryptography is splendid. Encrypt to your recipient's public key.

Problem:

Are you sure this is their key?


fairy
dust

Solution:

Find a person everyone trusts.

just trust

1500

people

APRIL 7, 2011 | BY CHRIS PALMER

Fully-qualified Nonsense in the SSL Observatory

Yesterday, I posted about how internet certification authorities will sign unqualified names, which have no meaning on the internet.

In addition to unqualified names being meaningless — or, worse than meaningless — there are also meaningless fully-qualified names. And, yes, CAs will sign those names too.

As you may know, the internet domain name system (DNS) has a hierarchical structure: at the top are the *top-level domains* (TLDs) like .com, .org, and .net. Additionally, each two-letter ISO country code like UK, JP, and CN is also a valid *country-code TLD* (ccTLD). Finally, there are the lesser-known TLDs like .mobi, .museum, and .int.

Although you can register most any name (that contains letters, numbers, dashes, and arguably underscores) *underneath* the TLDs, *the set of TLDs is fixed*. Although ICANN might

Every secure connection relies on 1500 entities not ever having made a critical error.

Summary

Cryptography is close to perfect

Everyone trusts 650 CAs perfectly

CAs sometimes make mistakes

“Implementation details”

Expectations about cert meaning

Who is responsible for validity?

Are intercept certs permitted?

My implementation is correct, some other people just don't understand what this system is for.

- implementers

Mitigation

How to deal with CA mistakes?

What about very large CAs?

Options limited by trust model

mozilla

Tom Lowenthal
tom@mozilla.com
@flamsmark