End-to-end Security and Privacy

What’s the big deal?

- E2E Security is NOT a “default” on the Internet despite decades of maturity

- if it were, we could have:
  - Internet-scale Object Security
    - IoT devices
    - mHealth
    - Smart-city infra.
  - Legal standards:
    - easy compliance
    - HIPAA
    - GDPR
  - Cyber Threat Intelligence
    - secured sharing
  - Active research
    - CCI funded
    - Invisible Security

- S/MIME spec written 20 years ago

why?

1) technical: usage limited to organizational boundaries
2) human: annoying to use for the everyday individual

**Solution**
- give email users a simple “ON switch” for secure email
  - with Cert Management System and MUA add-on
  - daneportal.net and Kurer

Secure Email is the launchpad to bring ubiquity to E2E security

Imagine the Internet before https ... that is where we stand for E2E

Secure Internet-scale Key-learning

biggest limitation:

Can’t cross organizational bounds

why?

1) security by public-key cryptography, but we can’t learn the public keys!

**Solution:** allow anyone to find any cert by putting them on:

Made possible using the protocol

DANE (RFC 6066)

DNS-based Authentication of Named Entities (RFC 6698)

Mature, robust, and decentralized

DANE key-learning solution

- One-click: Creates and serves DANE zone for zone admins
- Streamlined front-end lets users to add S/MIME certs

Delegation of responsibility:

- Admins manage their zones and users
- Email users manage their own certs

Key Design

Operational issues stymie interest and uptake

Overcoming them is daneportal.net

Challenge

Using DANE can be complicated

- How to operate the DANE zone?
- Users have many emails addresses!
- What if email users want to use their own key?

Secure Email

- Augmented with
  - Open-source add-on for popular MUAs
  - Outlook (Web/Client) and Thunderbird
  - S/MIME signing and encryption
  - DANE auto cert. discovery

Human-usuable S/MIME

USE CASE — encrypted email with Kurer

Bob uses student email: bob@someuni.edu

wants to message Alice so only she can read it

1. installs
2. composes email
3. toggles encryption
4. clicks send

Alice uses business email: alice@somecorp.org

1. installs
2. adds her priv. key
3. reads message like usual
4. opens/decodes

Kurer and DANEportal:
True Democratized End-to-end Security and Privacy for End-users

Authors: Tawhidul Minar Islam, Joshua Yuen, Pavan Kumar Dinesh, Tomofumi Okubo, Eric Osterweil

Affiliation: Measurable Security Lab, CS Dept., George Mason University

Title: Kurer and DANEPortal: True Democratized End-to-end Security and Privacy for End-users

email: the grandfather of messaging

- everyone uses it
- barely anyone secures it

넷플릭스: S/MIME

Kurer

Create and serve DANE zone for zone admins

Cert Management System

MUA add-on

daneportal.net

Solution

- allow anyone to find any cert by putting them on:

Made possible using the protocol

DANE (RFC 6066)

DNS-based Authentication of Named Entities (RFC 6698)

Mature, robust, and decentralized

DANE key-learning solution

- One-click: Creates and serves DANE zone for zone admins
- Streamlined front-end lets users to add S/MIME certs

Delegation of responsibility:

- Admins manage their zones and users
- Email users manage their own certs

Key Design

Operational issues stymie interest and uptake

Overcoming them is daneportal.net

Challenge

Using DANE can be complicated

- How to operate the DANE zone?
- Users have many emails addresses!
- What if email users want to use their own key?

Secure Email

- Augmented with
  - Open-source add-on for popular MUAs
  - Outlook (Web/Client) and Thunderbird
  - S/MIME signing and encryption
  - DANE auto cert. discovery

Human-usuable S/MIME

USE CASE — encrypted email with Kurer

Bob uses student email: bob@someuni.edu

wants to message Alice so only she can read it

1. installs
2. composes email
3. toggles encryption
4. clicks send

Alice uses business email: alice@somecorp.org

1. installs
2. adds her priv. key
3. reads message like usual
4. opens/decodes

Kurer and DANEPortal: True Democratized End-to-end Security and Privacy for End-users

Authors: Tawhidul Minar Islam, Joshua Yuen, Pavan Kumar Dinesh, Tomofumi Okubo, Eric Osterweil

Affiliation: Measurable Security Lab, CS Dept., George Mason University

Title: Kurer and DANEPortal: True Democratized End-to-end Security and Privacy for End-users

email: the grandfather of messaging

- everyone uses it
- barely anyone secures it

넷플릭스: S/MIME

Kurer

Create and serve DANE zone for zone admins

Cert Management System

MUA add-on

daneportal.net

Solution

- allow anyone to find any cert by putting them on:

Made possible using the protocol

DANE (RFC 6066)

DNS-based Authentication of Named Entities (RFC 6698)

Mature, robust, and decentralized