USING DANE AS THE FIRST STEPS TOWARDS GENERALIZABLE INTERNET-SCALE OBJECT-SECURITY: SECURE MESSAGING FOR TODAY AND TOMORROW

Minar Islam - tislam20@gmu.edu
Josh Yuen - jyuen2@gmu.edu
Pavan Kumar Dinesh - pdinesh@gmu.edu
Tomofumi Okubo - tomofumi.okubo@digicert.com
Eric Osterweil - eoster@gmu.edu
WHAT IS MOTIVATING OUR RESEARCH?

- Should we protect data in flight, at rest, or both?
  - Shouldn’t, actions be taken based on data, not (just) who transmits it?
- Can independent devices/entities auth. and encr. their messages to each other with 0-trust?
  - Say, a fire engine to a municipal traffic signal, and that signal to my POV Tesla?
- Transport-layer protections do not protect data
  - Shouldn’t the messages be protected too/instead?
- That is object-security, and it is different (and maybe more powerful) than transport-security
WHAT IS “OBJECT-SECURITY?”

• Well, first, what is a digital “object,” on the Internet?
  • It could be an image, a file, a message, an email, sensor reading, …

• The security/privacy we need for objects is different
  • “Objects” exist/persist “at rest,” i.e. beyond “in flight”
  • Example: I create a document, send it over WhatsApp to a friend, and then email it to a colleague
  • If the WhatsApp msg is encrypted, does that protect the doc at rest on my computer, or over email?

• But, the Internet doesn’t have a de facto way to do that today (i.e., an architecture)
  • Why can’t we encrypt/authenticate objects to anyone, except through WhatsApp, Signal, etc.?
• In this talk, we propose that we already have tomorrow’s object-security foundation from the Internet’s core, and it’s time to build on it!

DANE

• An Internet-scale object-security foundation will unlock protections for mHealth, V2X, Smart Cities, and more
THE FOUNDATION MUST SUIT ITS PURPOSE

• To know what Internet-scale object-security needs to be, we need to evaluate why object-security isn’t pervasive yet
• So, “why?” We’ve had mature crypto protections for years: S/MIME, PGP, etc.

What we already know:
our protections have been stymied by a simple limitation:
Our software can’t securely (inter-admin) learn the crypto keys

What we still need to know:
what are the fundamental needs + obstacles;
to be sure foundation will bear the Internet’s weight
Examples like IoT, mHealth, V2X, etc. show increasingly repeated requirements:
- Inter-organizational (e.g., entity at University A to entity at company B)
- Per-entity (e.g., device, user, etc.) E2E crypto at Internet-scale
- Usable tools
- Automation

An “architecture” should synthesize these
Same objects secure in and between apps!

Secure objects at rest!

Object-security extends from the core up to apps.
To do that, we have built a live experimental apparatus: secure email

Securing email will vault cybersecurity forward, but more than that it will prove the utility of the underlying architecture
- An email add-on called Kurer and a management portal at DANEportal.net
- Object format for the Internet (using PKCS7)!

These will let us evaluate the fundamental needs of Internet-scale security and privacy of digital objects (e.g., messages, files, etc.), at scale
INTERNET-SCALE OBJECT SECURITY REQUIREMENTS

• Recall our fundamental requirements (messaging platform, aside):
  • Inter-organization key learning
  • Per-user crypto key enrollment
  • Human-usable tools for e2e protections
  • Framework to enable security-automation

• DANEportal.net
  • Management of users’ DANE keys

• Kurer
  • User-side DANE software

S/MIME with DANE
DANEportal.net
Kurer MUA plugins
NEXT UP
Entity-Security / “invisible security”

Tools you can use, today!
WHAT ARE DANEPORTAL.NET AND KURER?

• DANEportal.net is where email users from any domain ("identity holders") can securely make their crypto keys **learnable**
  • Domain holders securely claim their zone (using ACME protocol)
  • DANE is managed for them
  • Email users, under a domain, create accounts and manage their own key life-cycles

[http://daneportal.net/](http://daneportal.net/)

• Kurer is an add-on/plugin for Mail User Agents (MUAs, Outlook and Thunderbird)
  • Email users install Kurer
  • Configure their crypto keys
  • And go secure... To anyone, anywhere, anytime

• Observation: secure email builds from core Internet security up to users
  • Ideally positioned to extended further... more later
• Create a portal user account

• Add your zone

• Claim your zone using ACME protocol to verify proof of administration

Verify Zone Claim

example.com verification challenge

To prove control over zone, insert the following token as a TXT record in the _acme-challenge.example.com dns zone and click "Verify" below:
cfa713d5f828e11eb6eb6e637d8bc25bdf

Cancel

Verify

Close
**DELEGATE FROM YOUR ZONE TO DANEPORTAL**

- Add NS and DS to your zone using your zone management tools
  - Zone cut at ":_smimecert"

![Zone management tools](image)
NOW, ADD USERS’ EMAIL ADDRESSES

- Users create DANEportal accounts

- Zone admins authorize portal users as “denizens”
  - i.e., email addresses under a zone

- Denizens are your email users
  - Users add S/MIME records to your DANE zone
  - Admins do not lose any control
EMAIL USERS CAN CREATE/MANAGE THEIR OWN CERTIFICATES

For now, toggle the **authorize switch** to the right and click
• Manage records by toggling its authorization state or deleting it permanently

• DANE allows “de-authorization” of keys
  • Not revocation, and faster

• For now, toggle the authorize switch to the right and click [Apply]
GETTING KURER ON OUTLOOK IS A SNAP!

Full install directions: https://kurer.daneportal.net/install
Hey, this message should be signed so you know I wrote it!

-Minar

This message has been signed using Kurer

Plaintext:

Hey, this message should be signed so you know I wrote it!

-Minar
• Automatically detect if incoming emails are encrypted or signed
• Simply click the text to automatically decrypt the email and view the plaintext
• New reply buttons with additional functionality
STATUS

• DANEportal.net is live, today
  http://daneportal.net/

• Kurer is in *alpha release*, for Outlook and Thunderbird
  https://kurer.daneportal.net/install
This technology will secure digital objects throughout cyberspace:

- Mobile Healthcare (mHealth), Smart and Connected Communities (SCC), 5G Internet of Things (IoT) security, Vehicle-to-Everything (V2X) communications, and much more.

Just like email, those disciplines will also need:

- Inter-organizational foundations
- Per-user E2E crypto, Internet-scale
- Human usable tools

Securing email with DANE paves the way to evolve protections from the Internet’s core:

- This work will evaluate in order to evolve protections that fit
- Deployable immediately

Next: Entity-Security... Developing a tool for Security, Privacy and Trust Enrollment (SPaTE)
THANK YOU!

EOSTER@GMU.EDU
Are our communications and data private on the Internet?

Well, maybe you’ve heard, no:

And so are your EMAILS!
TAKE AWAY FROM THAT...

• What did we see there (besides a mixed metaphor of mail vs. messaging)?
  • Privacy: People expect that even snail-mail, in meat-space, is private
• What did we not see there?
  • Authenticity: no one expected to verify the of sources of mail
• Cybersecurity and privacy on the Internet should be more advanced and automated than in meat-space
  • Drones & automobiles should be able to transact with each other
  • Doctors should be able to send health records to patients
  • …
• The Internet should enable this, but fundamental requirements have not been met
Examples like IoT, mHealth, V2X, etc. show increasingly repeated requirements:

- Inter-organizational (e.g., entity at University A to entity at company B)
- Per-entity (e.g., device, user, etc.) E2E crypto at Internet-scale
- Usable tools
- Automation

The foundations we need already operational in Internet’s core

- The Domain Name System’s Security Extensions (DNSSEC)
  - 16+ years, ~10^7 global zones, inter-org loosely-federated, etc.

- DNS-based Authentication of Named Entities (DANE)
  - General object-security, ~10 years, per-entity crypto, etc.
• Why not build cybersecurity / privacy protections from the top down?
  • Secure messaging works, right?
  • Why not build on blockchain?
  • Why not something else that fills a need?
• Internet needs an architecture for **cross-app** object-security
• Internet continuously proves things that “work” may not work **at scale**
• Internet’s needs **evolve**, and protections need to be **(re)evaluated**
• Building on Internet’s scalable core (protections) inherits versatility
  • DNSSEC has embodied scalable/usable protections for 16+ years
  • Email is inter-org, has been scalable/evolvable core protocol for decades, etc.
• S/MIME + DANE → scalable messaging and object security
PLAY WITH DANE AND ITS TOOLS

• DANE has been used in CTF at M3AAWG
  • https://www.m3aawg.org/

• libCanute: a reference library for DANE protocols
  • https://github.com/gmu-msl/canute

• DANEportal.net and Kurer will let you get started today
If Alice, Bob, and Chuck can securely find each others’ crypto keys, they can all communicate securely/privately!

But, even if Chuck has a key, Alice cannot securely/privately communicate with him!

Then, with DANE, Alice, Bob, and Chuck can provision their own crypto keys so they can securely find each others’ keys

First step: secure DNS with DNSSEC

How can we make everyone’s key globally learnable, securely?

Adversary fails!

Adversary wins!

Then, adversaries fail to intercept secure/private communications!
CREATE YOURSELF A USER ACCOUNT

• Click [ New User ]
• Enter desired credentials
• Click [ Create User ]
• Click [ OK ] to close modal

• This will be your portal/management account
• Every email user will need their own login
  • Third-party OAuth logins are a planned feature, as is automated bulk account creation
KURER FOR THUNDERBIRD

No-click solution for seamless DANE S/MIME
https://github.com/gmu-msl/kurer-thunderbird

Only one setting is really needed for now:
• Enter your private key and sending email address to allow signing your email
JUMP RIGHT IN TO SENDING SECURE EMAIL

- Use the Kurer popup to toggle signing and click send encrypted
  - The SIG tag on the icon means the email will be signed when sending