A Comparative Usability Study of Key Management in Secure Email

Scott Ruoti
Jeff Andersen, Tyler Monson, Daniel Zappala, Kent Seamons

THE UNIVERSITY OF TENNESSEE KNOXVILLE

BRIGHAM YOUNG UNIVERSITY FOUNDED BYU 1875 PROVO, UTAH

Motivation

- How does an IBE-based email system fare against a well implemented PGP-based email system?
- Two outcomes
    - Research results
    - A research platform

IBE—Identity-Based Encryption
PGP—Pretty Good Privacy

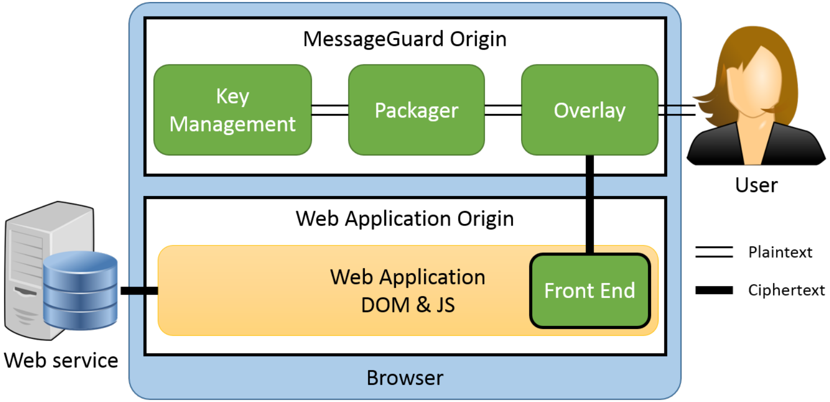
MessageGuard:
A Research Platform For Securing the Web

The Web

- Much of today’s software is on the Web
- Strong push for moving desktop software to the cloud
  - Software-as-a-Service (SaaS)
- Pros
  - Cheap
  - Scalable
  - Resilient
- Cons
  - Limited ability to configure
  - No control of own data

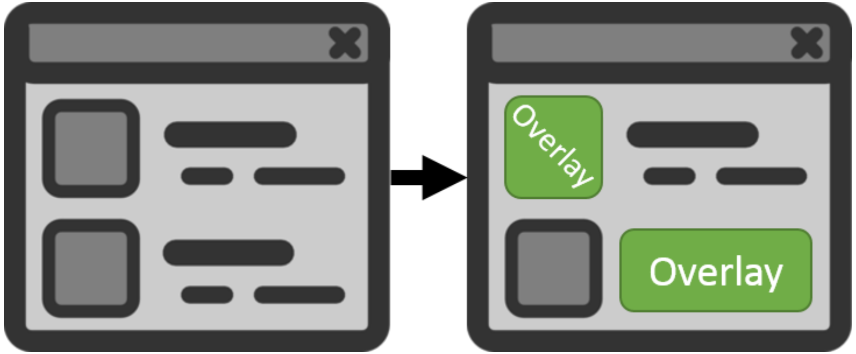
MessageGuard

- Retrofit websites/SaaS products to add security
  - Add end-to-end encryption
  - Verify signatures of content
- Does not require cooperation by the website/SaaS product
- Strong isolation from the underlying application



Afanasyev et al. *Content-Based Security for the Web*. NSPW 2016. ACM, 2016.
SaaS—Software as a Service

Security Overlays



- Replace portions of the interface with overlays
  - iFrame
- Author and view secure content in the overlay
- Visually seamless

Research Platform

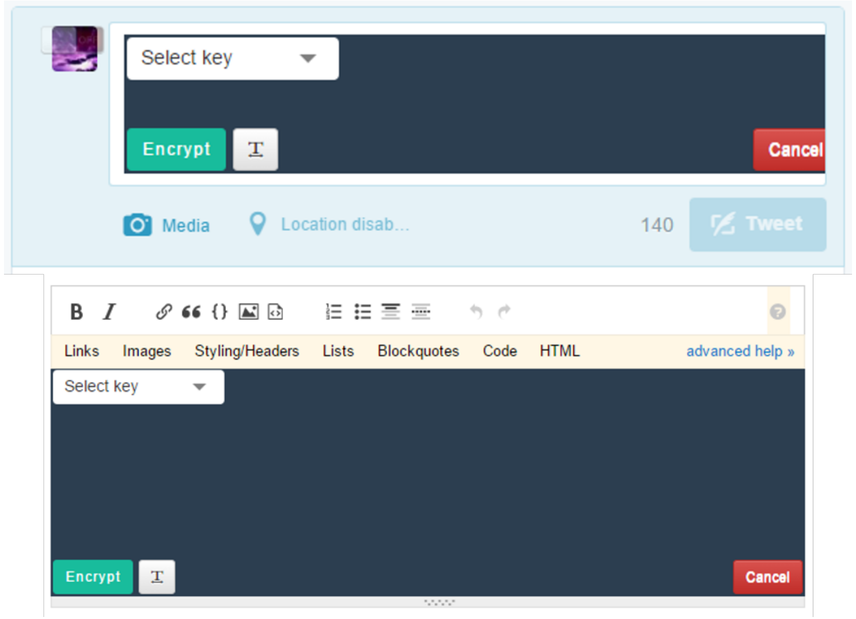
Framework

- Easy-to-modify
  - Pluggable
- Universal
  - Most websites
  - Desktop and mobile
- Fast

Benefits

- Accelerate the creation of functional prototypes
  - Simplifies creating prototypes for A/B testing
- Provides an easy way to share research results

Example Systems



- Private Facebook Chat
  - Robinson et al., 2012
- Pwm 2.0
  - Ruoti et al., 2016
- Short-lived keys
  - Monson et al., 2018
- This work

Robison et al. *Private Facebook Chat*. SocialCom 2012.
Ruoti et al. *Private Webmail 2.0: Simple and Easy-to-Use Secure Email*. UIST 2016.
Monson et al. *A Usability Study of Secure Email Deletion*. EuroUSEC 2018.

Research Opportunities

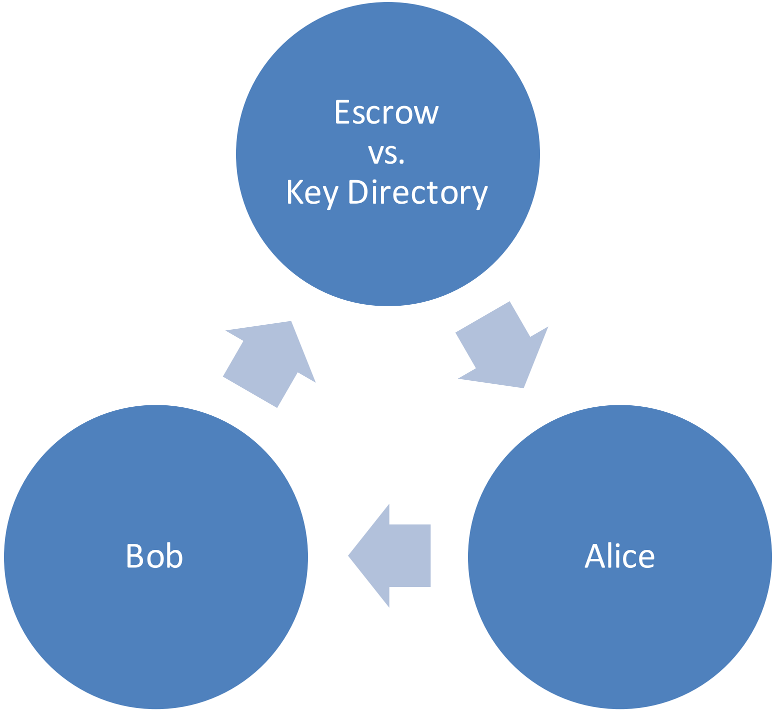
- Security researchers
  - Easily conduct usability studies
  - Key management
  - Messaging protocols
- Usability researchers
  - Test fully-implemented systems
  - Trustworthy interfaces
  - Avoiding mistakes

Available now at
https://messageguard.io

Comparing Key Management in Secure Email

IBE vs. PGP

- IBE consistently outperforms PGP
- Reasons to questions this gap
  - Poorly designed PGP systems
  - Emergence of public key directories (PKD)
- Prior work is insufficient to answer this question


Escrow
vs.
Key Directory

Bob

Alice

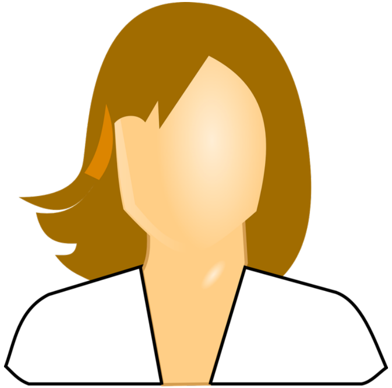
Study Design

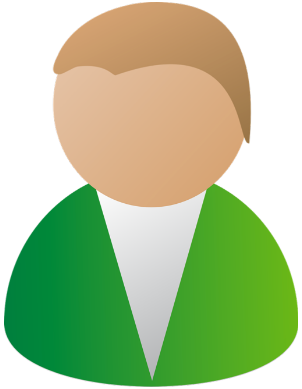
- Use MessageGuard to create email prototypes that differ only in key management
  - IBE, PKD, and Passwords
- Leverage standard metrics
- Use a two-person study methodology

IBE—Identity-Based Encryption
PKD—Public Key Directory

Two-Person Methodology

- Two roles
  - Johnny—initiator
  - Jane—initiated
- Simple task
  - Helping with taxes
- Within-subject



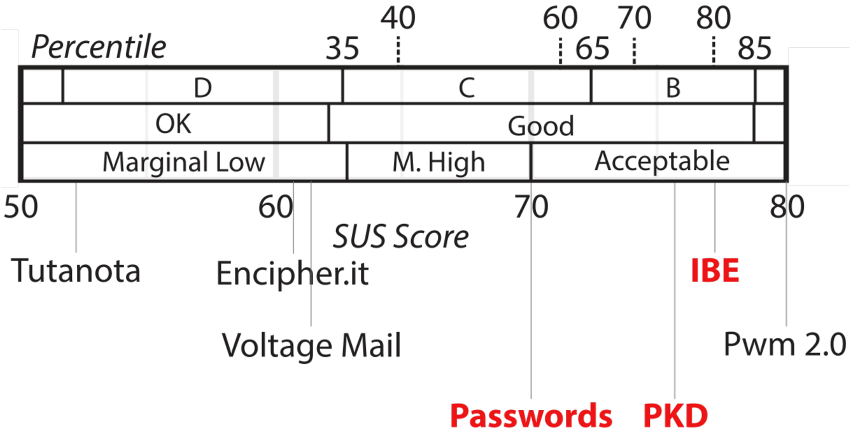


Demographics

- 94 total participants
  - Largest secure email study
- 50/50 gender split
- Most were undergraduate students
  - Attempted to recruit non-students, but failed
  - Not all were from our university

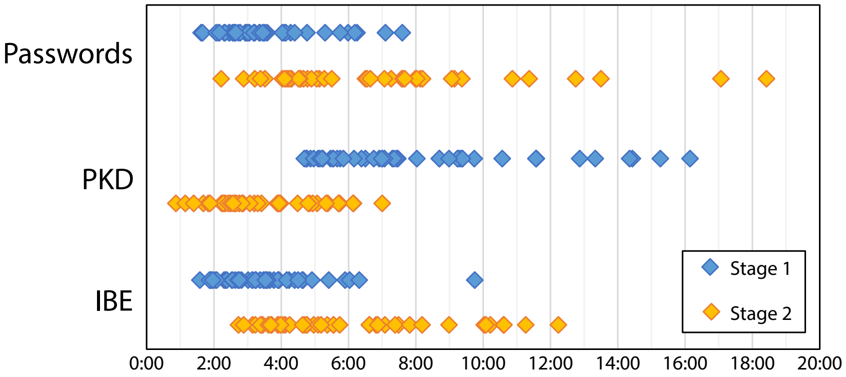
Results—Perceived Usasbility

- IBE and PKD performed similarly
- Passwords performed the worst
- MessageGuard-based systems outperformed other similar systems



IBE—Identity-Based Encryption
PKD—Public Key Directory
Ruoti et al. *Private Webmail 2.0: Simple and Easy-to-Use Secure Email*. UIST 2016.

Results—Time



- No difference in overall time
- PKD takes longer to send first encrypted email
- *"I am more motivated (i.e., I can more readily see the need) to install the app if the encrypted message is already sitting there in my inbox. Also, the fewer emails I have to send/receive the better."*

Results—Other

- Understanding
  - IBE and PKD performed poorly
  - Passwords were intuitive
- Favorite System
  - Split between the three
  - Changed with understanding

- Passwords
  - Why not just use the out-of-band channel for communication?
  - *“It was way lame that I had to call him because I might as well have just given him the info that way. . . . If I'm gonna communicate with them through email, it's because I want to do it through email, not through a phone call.”*

IBE—Identity-Based Encryption
PKD—Public Key Directory

Limitations

- Impossible to remove all confounding factors
- Laboratory study
- Focused on first-time use
- Non-representative demographic

SUMMARY

Summary

- MessageGuard is a research platform for securing the Web and SaaS
  - Many interesting research questions to be explored
- Compared the usability of key management in secure email
  - Gap between IBE and PKD is minimal
- Data and code available at https://messageguard.io/

SaaS—Software-as-a-Service
IBE—Identity-Based Encryption
PKD—Public Key Directory

Thank you