"Private Webmail 2.0: Simple and Easy-to-Use Secure Email"

S. Ruoti, J. Andersen, T. Hendershot, D. Zappala, K. Seamons

29th ACM Conference on User Interface Software and Technology, 2016

Francesco Mucci

Corso di Laurea Magistrale in Informatica

Interazione Uomo Macchina

2016-2017

UNIVERSITÀ
DEGLI STUDI
FIRENZE

Visione d'insieme

Internet Security Research Lab (Brigham Young University, Utah).

- Usable security.
- Email sicure ed usabili: problema aperto da almeno quindici anni.
- Focus su usabilità per nuovi utenti e non esperti.

Pwm 1.0

Webmail sicura, integrata.

Pwm 2.0

Quattro modifiche all'interfaccia per migliorare l'usabilità.

Insicurezze delle email

- Email providers (Gmail, Hotmail, etc.) possono leggere email non in transito.
- Alcuni email provider comunicano tra loro in chiaro.
- I link di comunicazione, anche se sicuri (TLS), sono aperti ad attacchi.

Email sicura

Cifra il messaggio prima di inviarlo (Crittografia end-to-end).

Stato dell'arte delle email sicure

- Secure Email Depots
- PGP (Pretty Good Privacy)
- S/MIME (Secure/Multipurpose Internet Mail Extension)

Nessuno dei tre è indirizzato all'utente medio di Internet.

Usabilità delle email sicure

Valutazione di PGP 5.0 (1999)

A. Whitten, J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0", *8th USENIX Security Symposium*.

- 50% fallisce nel set-up.
- 33% riesce ad inviare messaggi cifrati.

Valutazione di Mailvelope (2015)

Un moderno client PGP.

- 10% riesce ad usarlo con successo.

Obiettivo della ricerca

Rendere le email sicure usabili per l'utente medio.

"Security is only as good as its weakest link, and people are the weakest link in the chain"

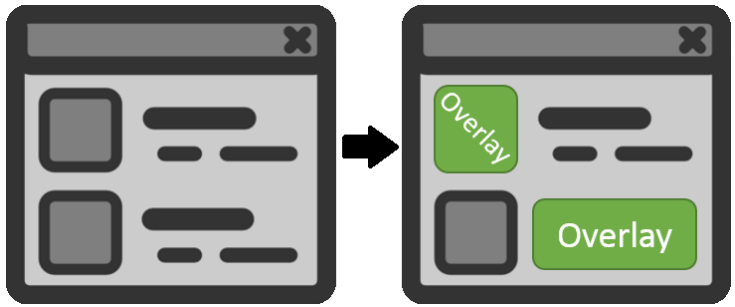
Strategia

Rilassare i requisiti di sicurezza al fine di ottenere maggiore usabilità.

- Sistemi teoricamente meno sicuri,
- ma più sicuri dal punto di vista pratico.

Private Webmail (Pwm) 1.0

1. Integra email sicura ad un sistema di webmail esistente (Gmail).
   - Security-overlays che visualmente si integrano con l'interfaccia. (Gli utenti sono resistenti ai cambiamenti, non amano i depot).

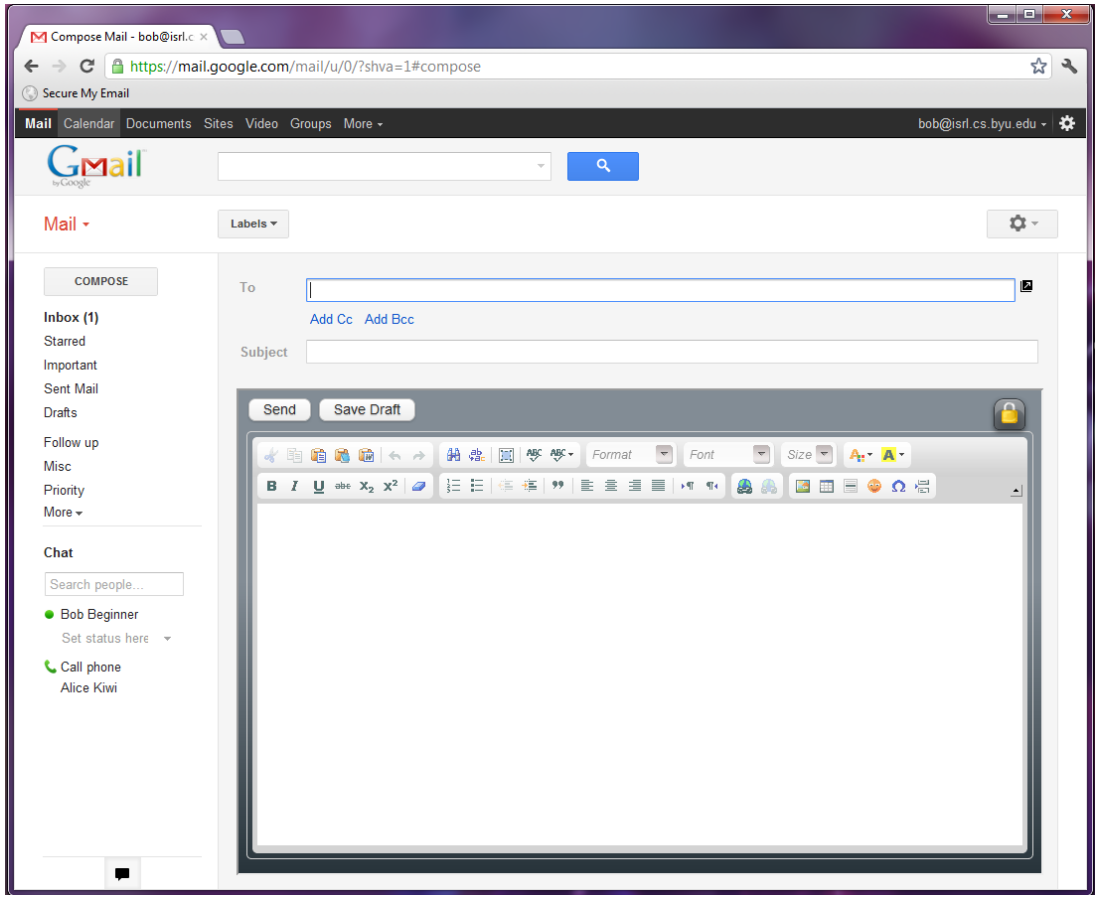


2. Nasconde i dettagli di sicurezza.
   - Cifratura automatica.
   - Gestione delle chiavi automatica.

Risultati dei test

- Ottimi punteggi di usabilità.
- $\sim$ 100% hanno usato il sistema con successo.

Private Webmail (Pwm) 1.0



Oppurtunità di miglioramento:

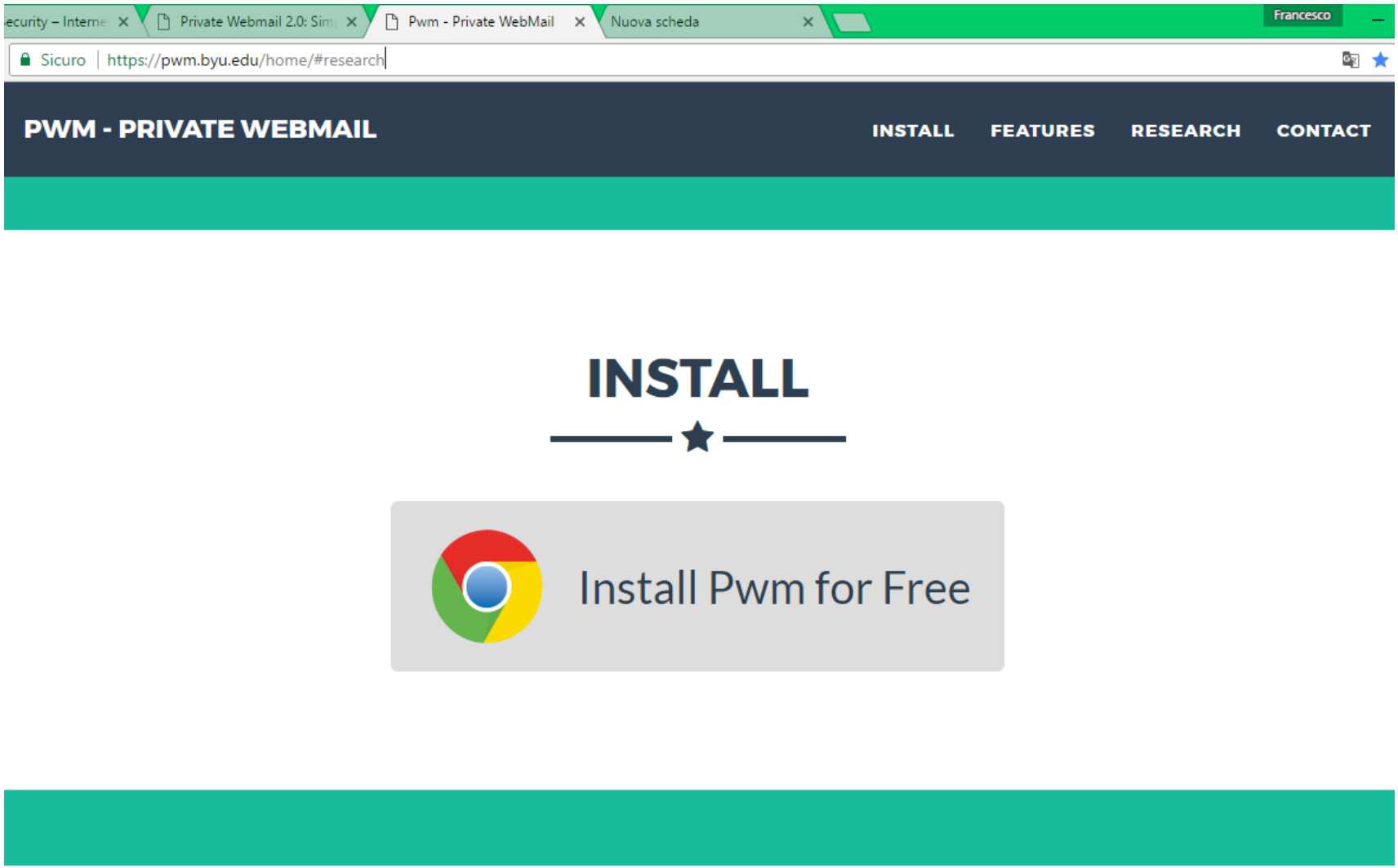
- Frequenza di errori.
- Fiducia dell'utente nel sistema.

Strategia di sviluppo

Miglioramento iterativo.

1. Raccolta idee.
2. Cognitive walkthroughs.
3. Testare le idee in studi su piccola scala.

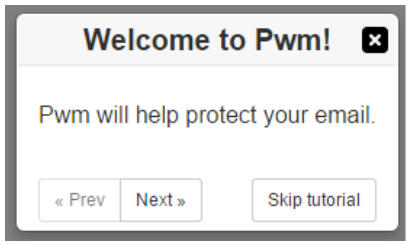
Miglioramento di Usabilità: "Look and Feel" sito web

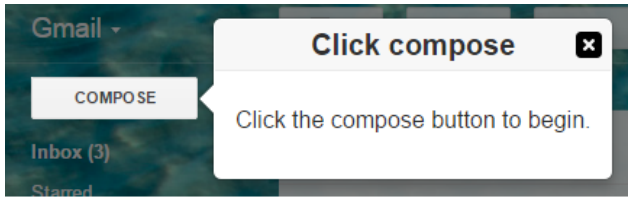


Sito professionale $=+$ fiducia.

Miglioramento di Usabilità: Tutorials

Context-sensitive in-line tutorial.

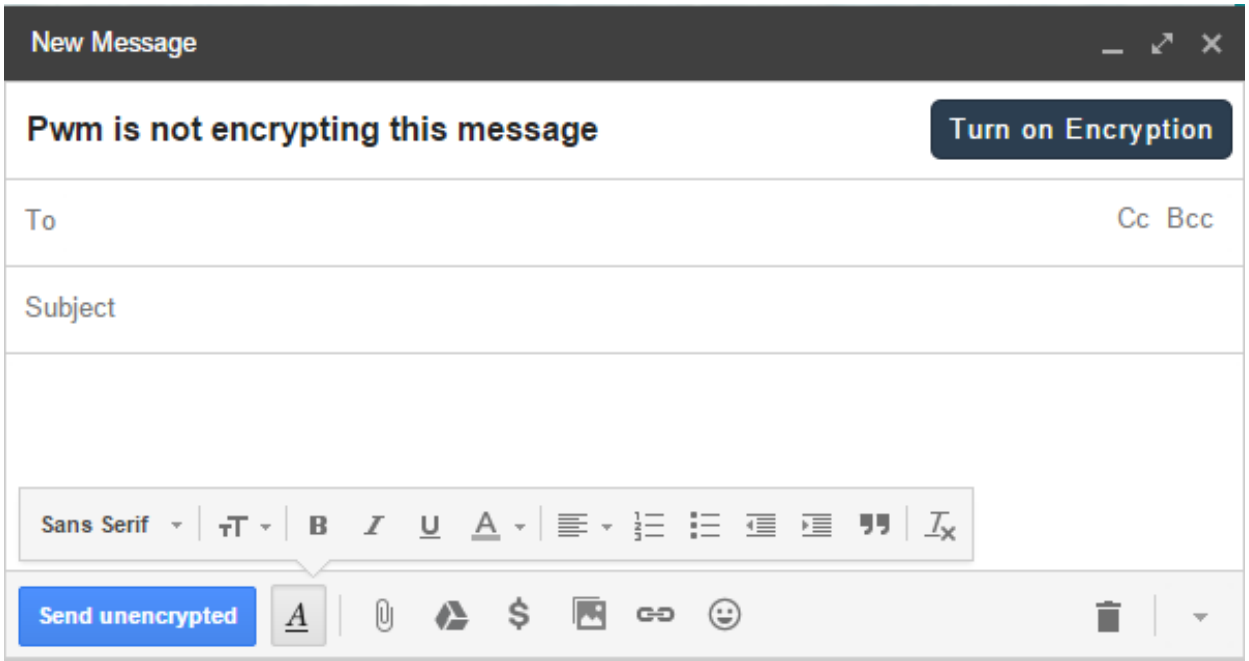




+ Context sensitive ⇒ più visualizzazioni ⇒ meno errori.
+ Spiegano concetti fondamentali crittografia ⇒ incremento fiducia.

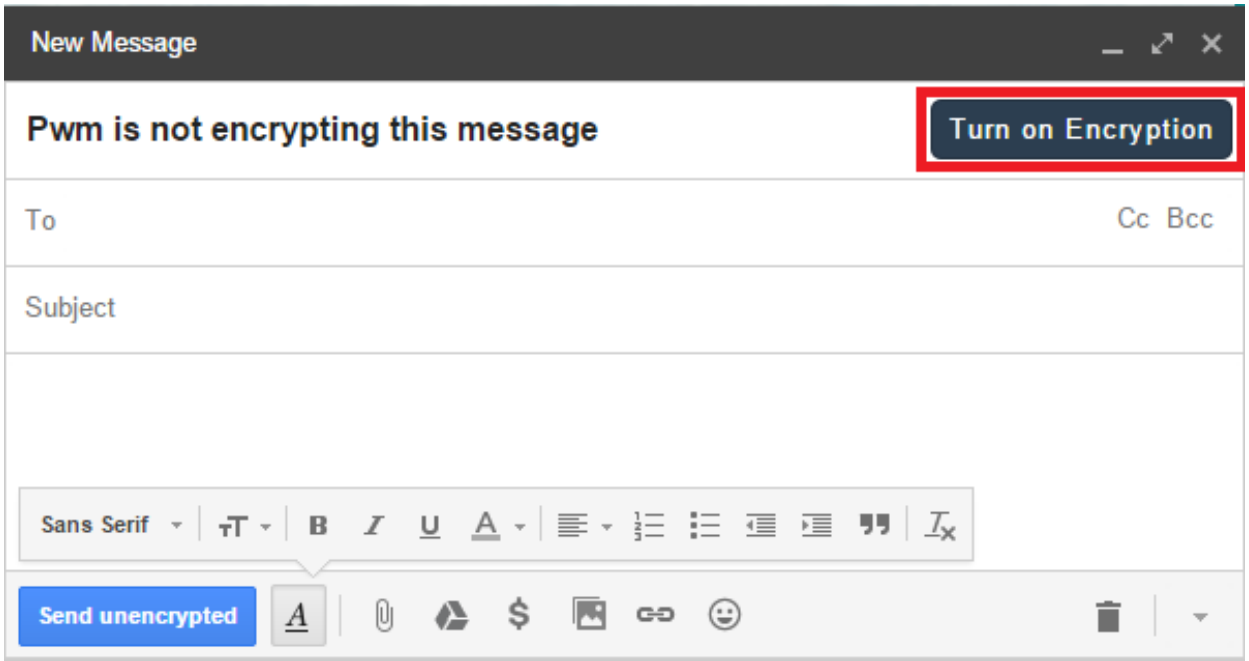
Miglioramento di Usabilità: Interfaccia di Composizione

Interfaccia di composizione in Pwm 2.0 prima di attivare la cifratura.



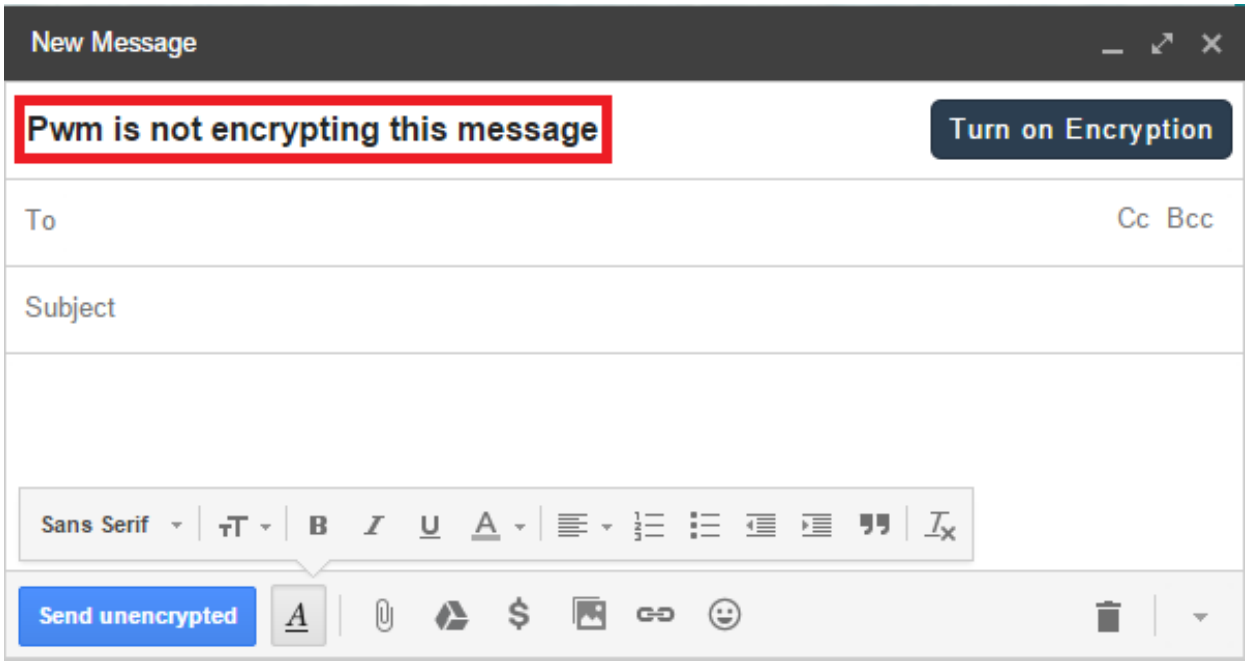
Miglioramento di Usabilità: Interfaccia di Composizione

Interfaccia di composizione in Pwm 2.0 prima di attivare la cifratura.



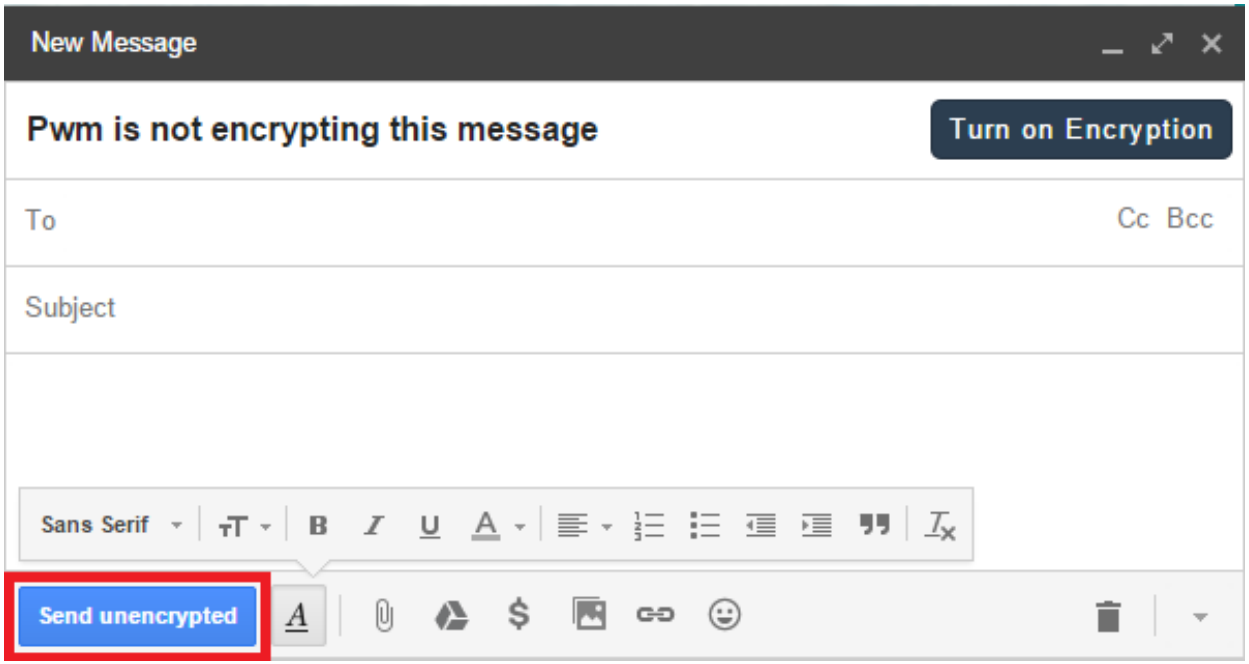
Miglioramento di Usabilità: Interfaccia di Composizione

Interfaccia di composizione in Pwm 2.0 prima di attivare la cifratura.



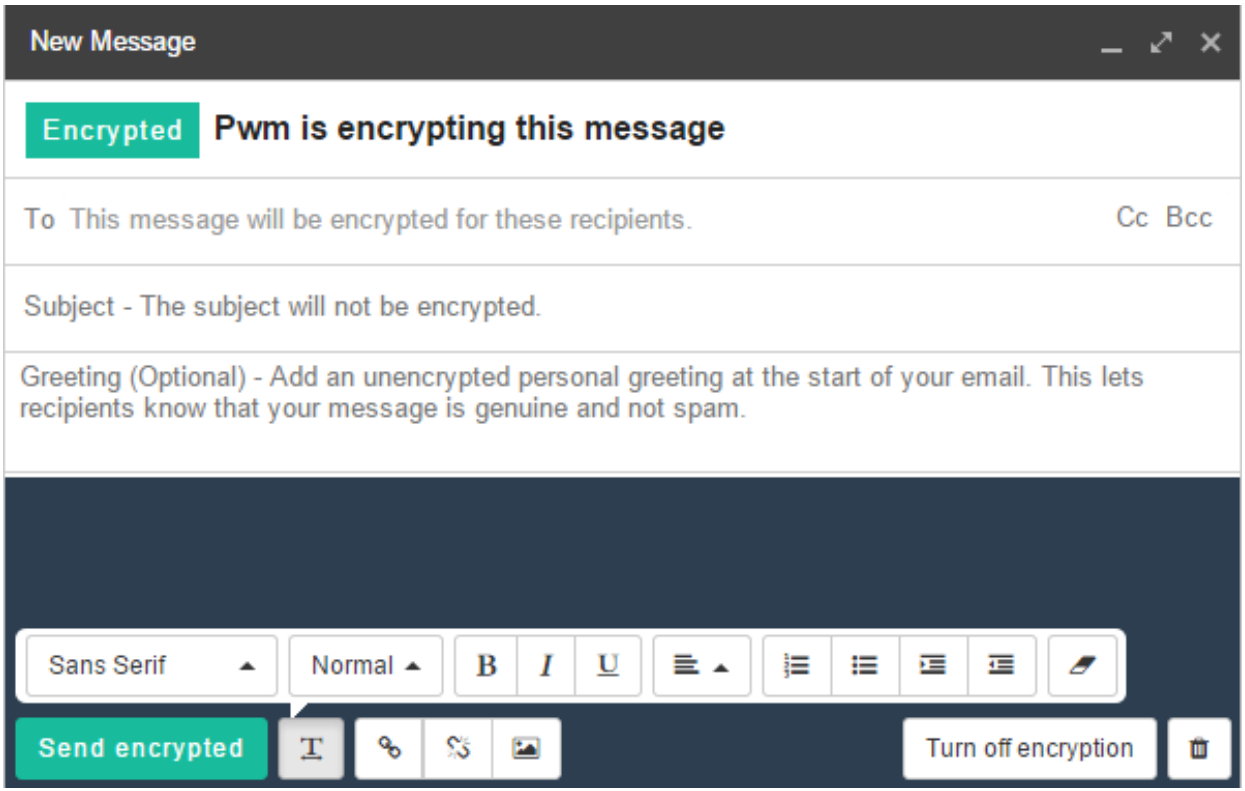
Miglioramento di Usabilità: Interfaccia di Composizione

Interfaccia di composizione in Pwm 2.0 prima di attivare la cifratura.



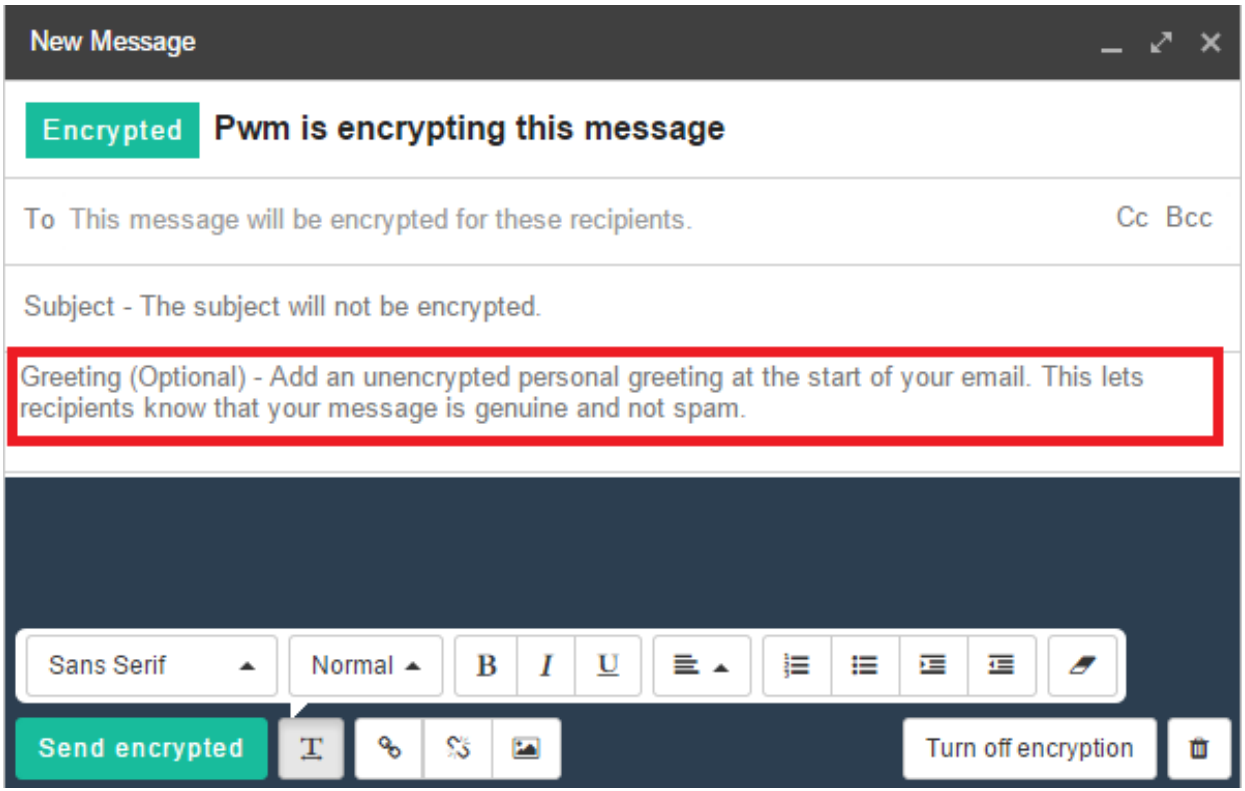
Miglioramento di Usabilità: Interfaccia di Composizione

Interfaccia di composizione in Pwm 2.0 dopo aver attivato la cifratura.



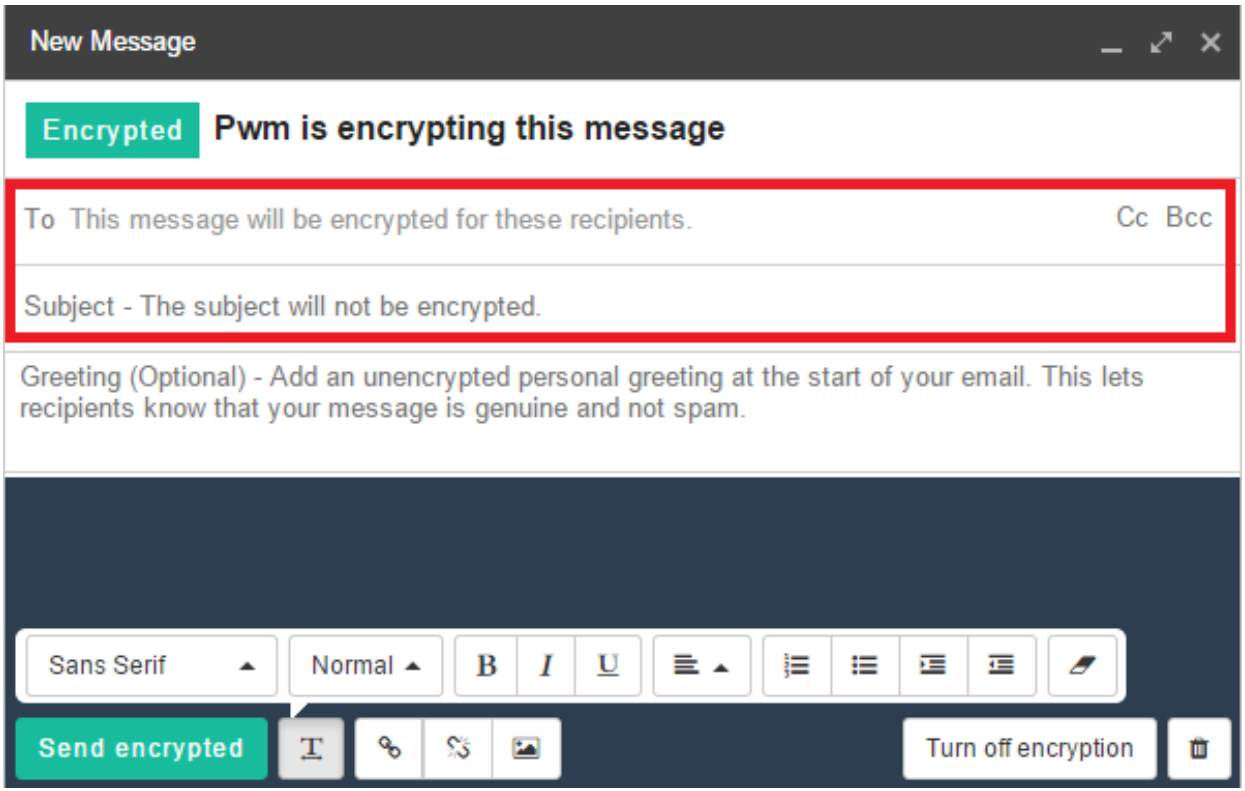
Miglioramento di Usabilità: Interfaccia di Composizione

Interfaccia di composizione in Pwm 2.0 dopo aver attivato la cifratura.



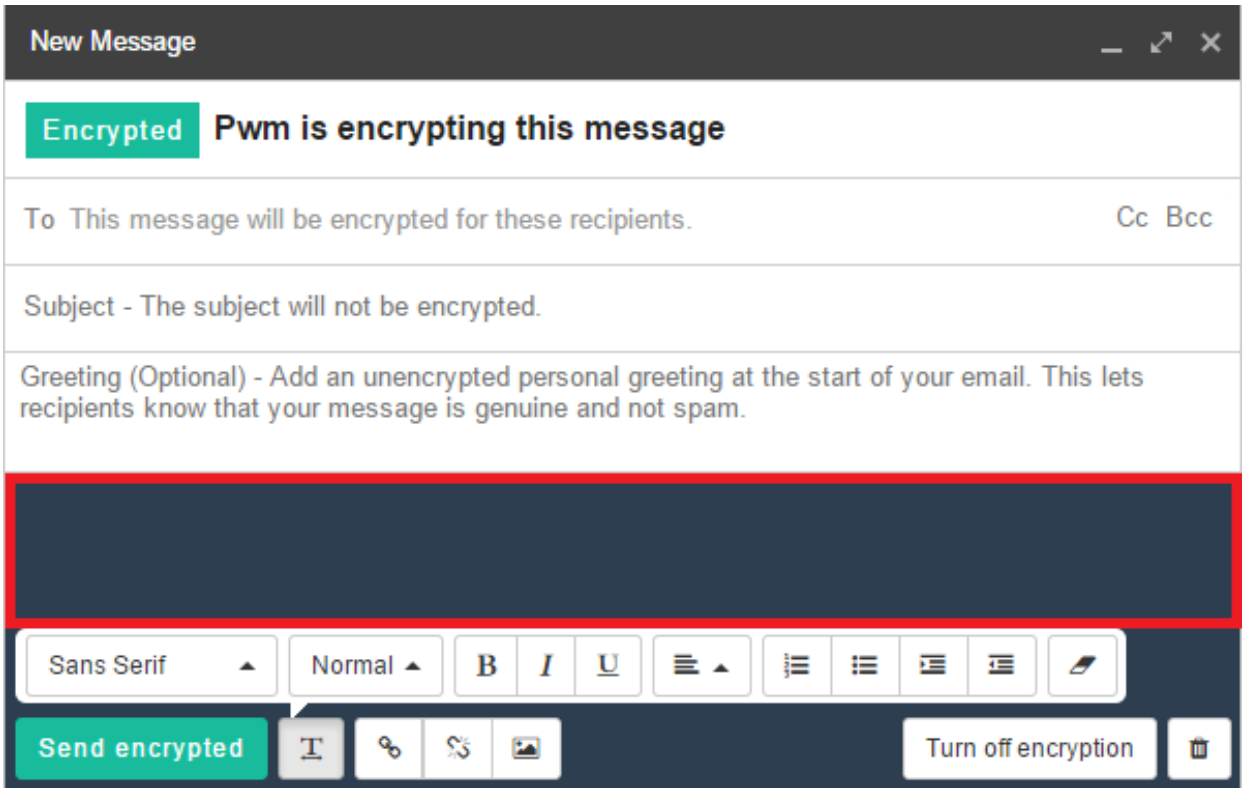
Miglioramento di Usabilità: Interfaccia di Composizione

Interfaccia di composizione in Pwm 2.0 dopo aver attivato la cifratura.



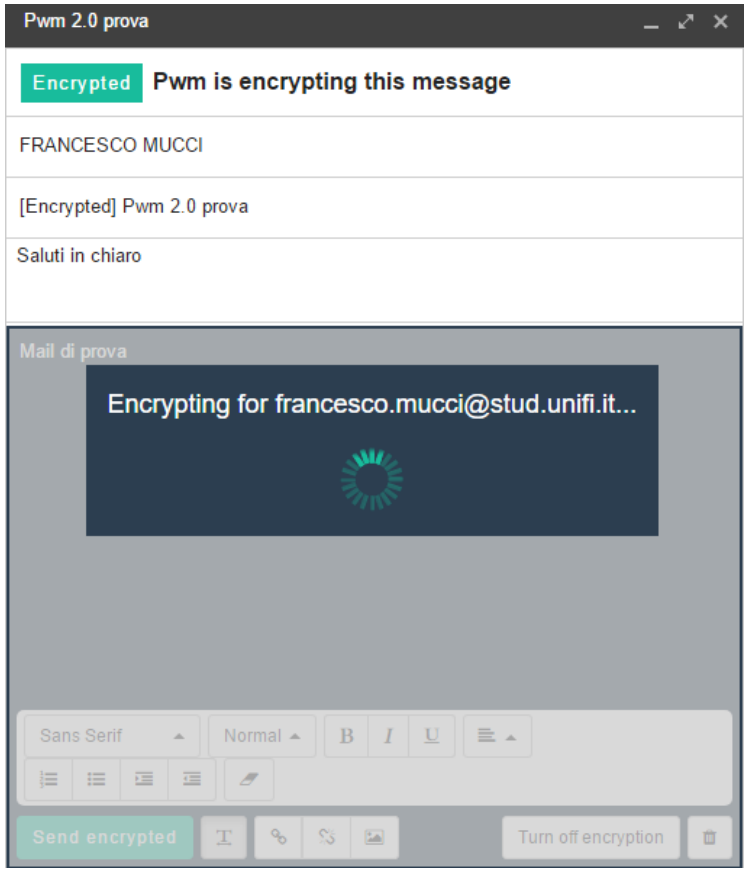
Miglioramento di Usabilità: Interfaccia di Composizione

Interfaccia di composizione in Pwm 2.0 dopo aver attivato la cifratura.



Miglioramento di Usabilità: Cifratura Ritardata

Ritardo artificiale nella cifratura di 0.75 secondi.



Aumenta la fiducia degli utenti nel fatto che Pwm faccia qualcosa per proteggere i messaggi.

User Study

- 51 partecipanti reclutati per "migliorare le email".
- Due scenari con varie task da completare.
  1. Completare un processo di assunzione inviando dati sensibili via mail.
  2. Inviare credenziali di log-in per la carta di credito al proprio compagno/a.
- Utenti interagiscono via email con uno dei coordinatori.

Obiettivo: ottenere dati quantitativi e qualitativi per valutare l'usabilità di Pwm 2.0.

Risultati di usabilità

Usabilità percepita: metrica SUS (System Usability Scale).

- 10 affermazioni valutate da 1 (strongly disagree) a 5 (strongly agree).
- J. Brooke, "Sus-a quick and dirty usability scale", *Usability evaluation in industry*, 1996.

SUS Scores

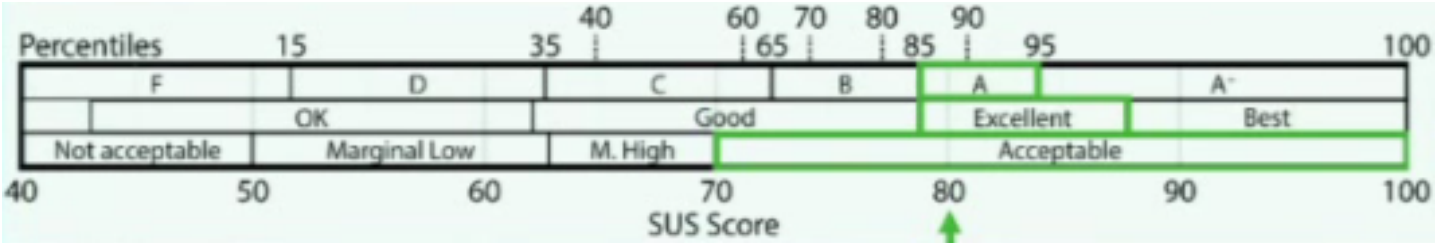
- Pwm 1.0: 74.2.
- Pwm 2.0: 80.0.

Risultati di usabilità

SUS Scores

- Pwm 1.0: 74.2.
- Pwm 2.0: 80.0.

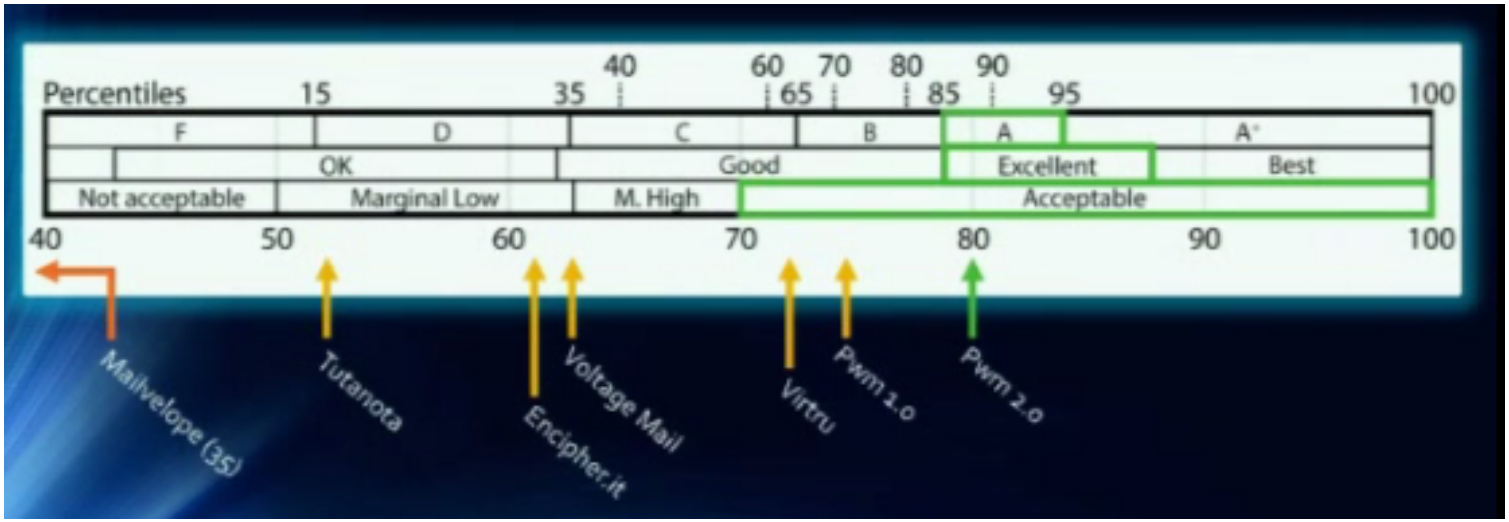
- A. Bangor, P. Kortum, and J. Miller, "Determining what individual sus scores mean: Adding an adjective rating scale", *Journal of Usability Studies*, 2009.



Risultati di usabilità

SUS Scores

- Pwm 1.0: 74.2.
- Pwm 2.0: 80.0.



Risultati relativi al numero di errori

- Registrazioni video: registrati i task in cui gli utenti hanno inviato informazioni sensibili in chiaro.

Task fallite (%)

- Pwm 1.0: 10%
- Pwm 2.0: 2%

Su 306 Task, solo 6 eseguite in modo non corretto.

Risultati relativi alla visione dei tutorial

- Registrazioni video: tracciato il numero di interazioni con i tutorial.

Partecipanti (%) che hanno visionato interamente i tutorial

- Introduzione: 92%
- Lettura: 92%
- Composizione: 54%

Grosso miglioramento rispetto a Pwm 1.0, dove quasi nessuno aveva visionato i video-tutorial.

Risultati di comprensione dei principi crittografici

- Questionario sulle proprietà crittografiche.

Partecipanti (%) che hanno risposto correttamente alle domande

- Confidenzialità: 83%
- Autenticazione: 62%
- Integrità: 75%

Miglioramento rispetto a Pwm 1.0, anche con domande più stringenti.

Risultati relativi al gradimento degli utenti

- Questionario sull'esperienza.

Partecipanti (%) che erano concordi con le affermazioni

- *"I want to start using Pwm"*: 82%
- *"I would use Pwm with my friends and family"*: 73%
- *"My friends and family could easily start using Pwm"*: 90%

Revisione della metodologia per lo user study

- S. Ruoti et al., "We're on the Same Page: A Usability Study of Secure Email Using Pairs of Novice Users", *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*.

Approccio "a due persone"

Due conoscenti, inesperti del sistema, comunicano liberamente ed iniziano ad usare Pwm. Interpretano ruoli diversi:

- Johnny: inizia lo scambio di messaggi ed introduce a Pwm.
- Jane: riceve una mail da Johnny e viene introdotto a Pwm.

Problemi di Sicurezza di Pwm 2.0

Sistema è aperto ad "impersonation-attack"

Malware diffuso tramite bookmarklet che emula Pwm

$\Rightarrow$ Men-in-the-middle.

Threat Model considerato: attaccante onesto-ma-curioso.

Sviluppi Futuri

Pwm rispetto a PGP:

- minore sicurezza teorica
- maggiore sicurezza pratica

- Applicare le lezioni apprese da Pwm per incrementare l'usabilità relativa di sistemi PGP-based.
- Rafforzare la sicurezza di Pwm mantenendo il livello di usabilità raggiunto.

Conclusioni

- Il problema delle email sicure ed usabili è problema aperto da molto tempo.
- Pwm mira a rendere le email sicure usabili per utenti inesperti.
- Pwm 2.0 ha ricevuto il più alto punteggio di usabilità tra tutti i sistemi di email sicure testati del gruppo di ricerca.

Bibliografia

- S. Ruoti, J. Andersen, T. Hendershot, D. Zappala, K. Seamons, "Private Webmail 2.0: Simple and Easy-to-Use Secure Email", *29th ACM Conference on User Interface Software and Technology (UIST)*, 2016.
- S. Ruoti, J. Andersen, S. Heidbrink, M. O'Neilly, E. Vaziripour, J. Wu, D. Zappala, K. Seamons, "We're on the Same Page: A Usability Study of Secure Email Using Pairs of Novice Users", *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*, 2016.
- S. Ruoti, N. Kim, B. Burgon, T. van der Horst, K. Seamons, "Confused Johnny: when automatic encryption leads to confusion and mistakes", *Proceedings of the Ninth Symposium on Usable Privacy and Security, Article No. 5, (SOUPS)*, 2013.

Grazie per l'attenzione.

Transpost Layer Security (TLS)

Protocollo crittografico erede di Secure Socket Layer (SSL).

TLS fornisce

1. Connessione privata tra client e server:
   - crittografia simmetrica (TLS Handshake $\rightarrow$ Shared Secret).
2. Autenticazione delle parti:
   - crittografia a chiave pubblica.
3. Integrità dei dati:
   - message integrity check usando message authentication code

Approfondimento di "Insicurezze delle email".

Stato dell'arte delle email sicure (approfondimento)

Secure email depots

Deposito da cui mandare e ricevere email sicure.

- Necessario account $\rightarrow$ non comodo.
- Non è possibile inviare mail sicure a chi non è registrato.

Stato dell'arte delle email sicure (approfondimento)

PGP (Pretty Good Privacy)

Sistema di cifratura asimmetrica.

- "Web of Trust" per verificare l'identità dei proprietari delle chiavi pubbliche.
- Per utenti inesperti è abbastanza ingestibile.

Stato dell'arte delle email sicure (approfondimento)

S/MIME (Secure/Multipurpose Internet Mail Extension)

Sistema di cifratura asimmetrica.

- Chiavi pubbliche sono contenute in certificati firmati da una Autorità Certificante (CA).
- Per utenti inesperti difficile acquisire ed usare certificati firmati.

Dettagli tecnici Pwm 1.0: Easy set-up

Browser extension

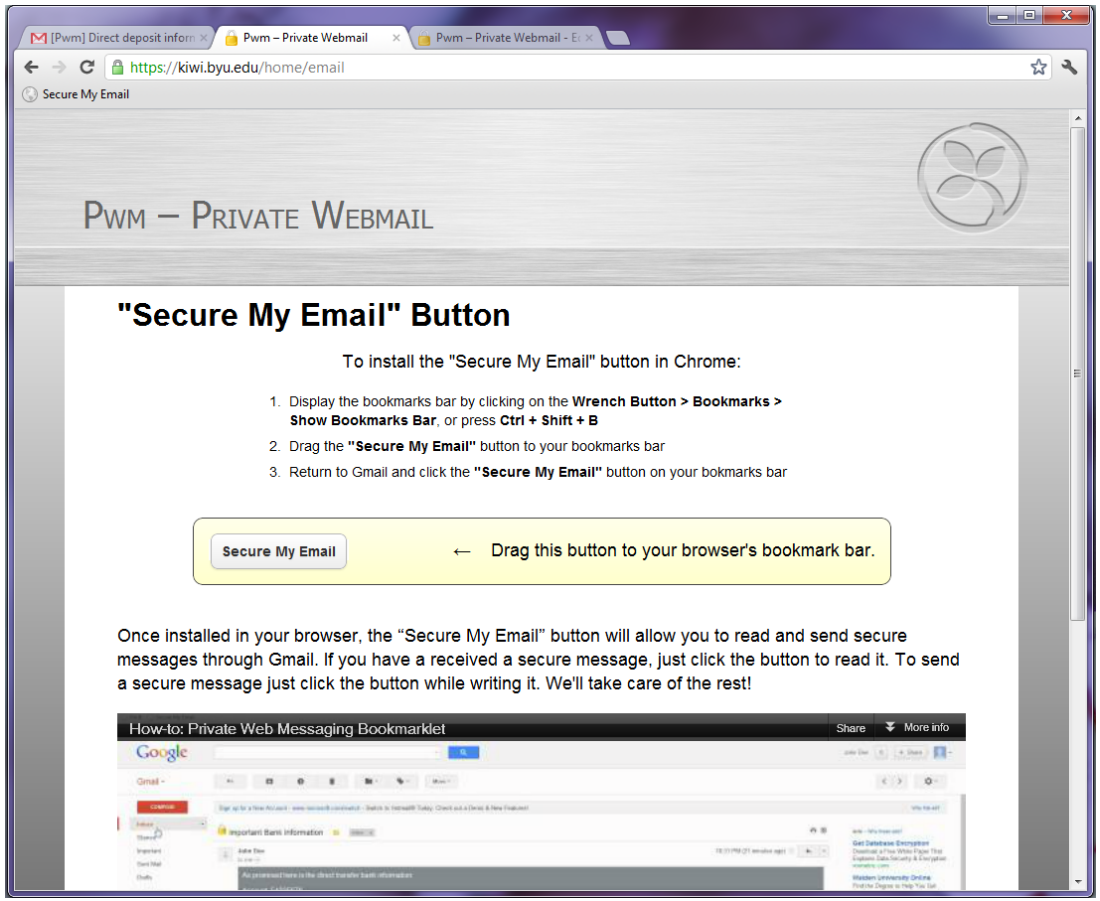
- Sempre in esecuzione.
- Presente solo in 1.0

Bookmarklet

Browser bookmark che contiene JavaScript invece di un URL.

- Bottone "Secure my Email" (va attivato ogni volta).
- Set-up facile e veloce.

Dettagli tecnici Pwm 1.0: Easy set-up



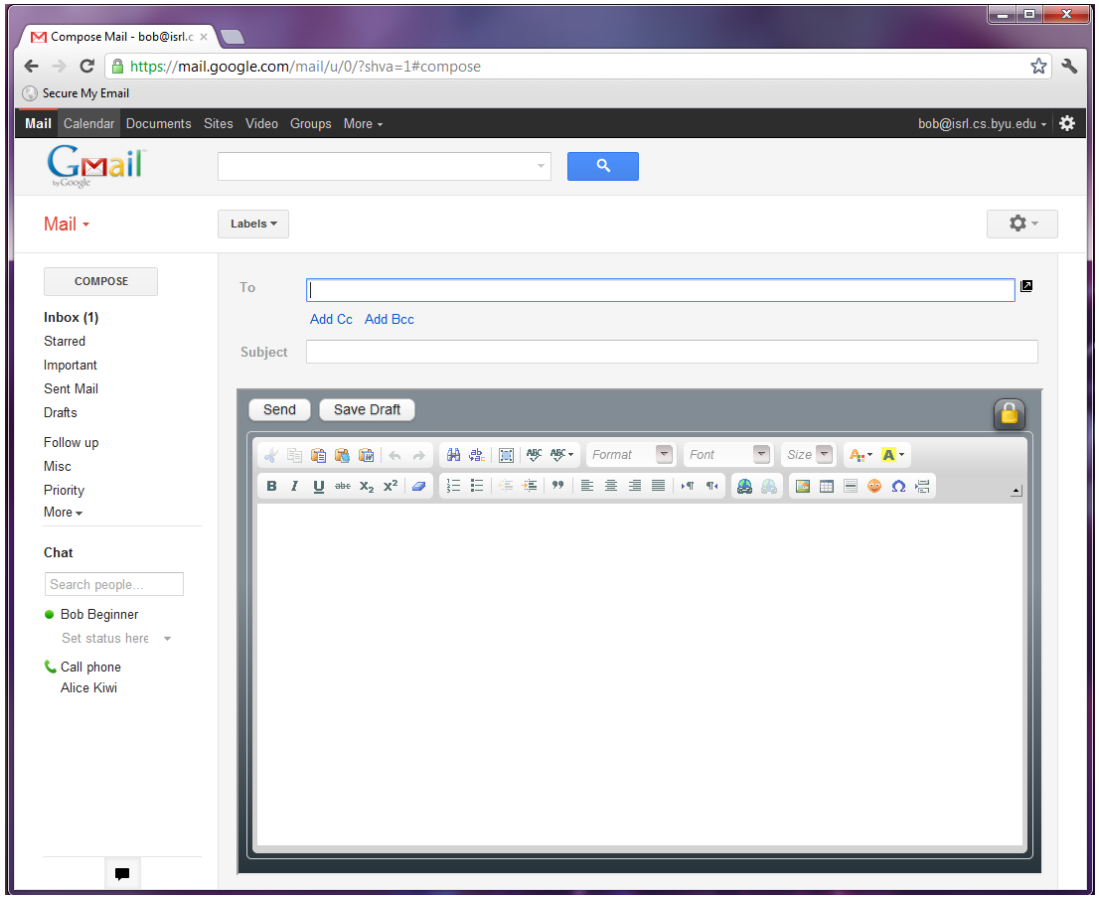
Approfondimento di "Private Webmail (Pwm) 1.0".

Dettagli tecnici Pwm 1.0: Security Overlays

Permettono integrazione dell'interfaccia.

- Implementati tramite iFrame.
- Gmail non può accedere al loro contenuto.
- Cifrano tutte le informazioni prima della loro trasmissione.
- Visivamente distinguibili in 2.0.

Dettagli tecnici Pwm 1.0: Security Overlays



Approfondimento di "Private Webmail (Pwm) 1.0".

Dettagli tecnici Pwm 1.0: Key-mgmt and Authentication Overlay

Ottiene e memorizza tutte le chiavi crittografiche. Gestisce ogni autenticazione necessaria per ottenerle.

Key-server

Gestisce e deriva a partire da email (identity-based cryptography) le chiavi. L'overlay ci interagisce per ottenere le chiavi.

+ Non necessario distribuire le chiavi pubbliche.
+ L'utente non può perdere le chiavi.
+ Chiavi portabili.
+ Key-mgmt invisibile ed automatizzato.
+ Overlay blocca scripts di webmail provider che cercano di accedere alle chiavi.
  - Key-server ha accesso alle chiavi private.

Dettagli tecnici Pwm 1.0: Key-mgmt and Authentication Overlay

Ottiene e memorizza tutte le chiavi crittografiche. Gestisce ogni autenticazione necessaria per ottenerle.

Simple Authentication for the Web (SAW)

Autenticazione necessaria a recuperare la chiave privata dal Key-server.

1. Pwm invia richiesta HTTP di autenticazione cifrata con TLS a SAW-server.
2. SAW-server genera token, lo divide in due.
   - Una parte a Pwm.
   - Una parte all'account mail che è stato autenticato.
3. Pwm recupera la parte mancante del token: ottiene la chiave privata.

Forma di Email-based identification and authentication (EBIA).

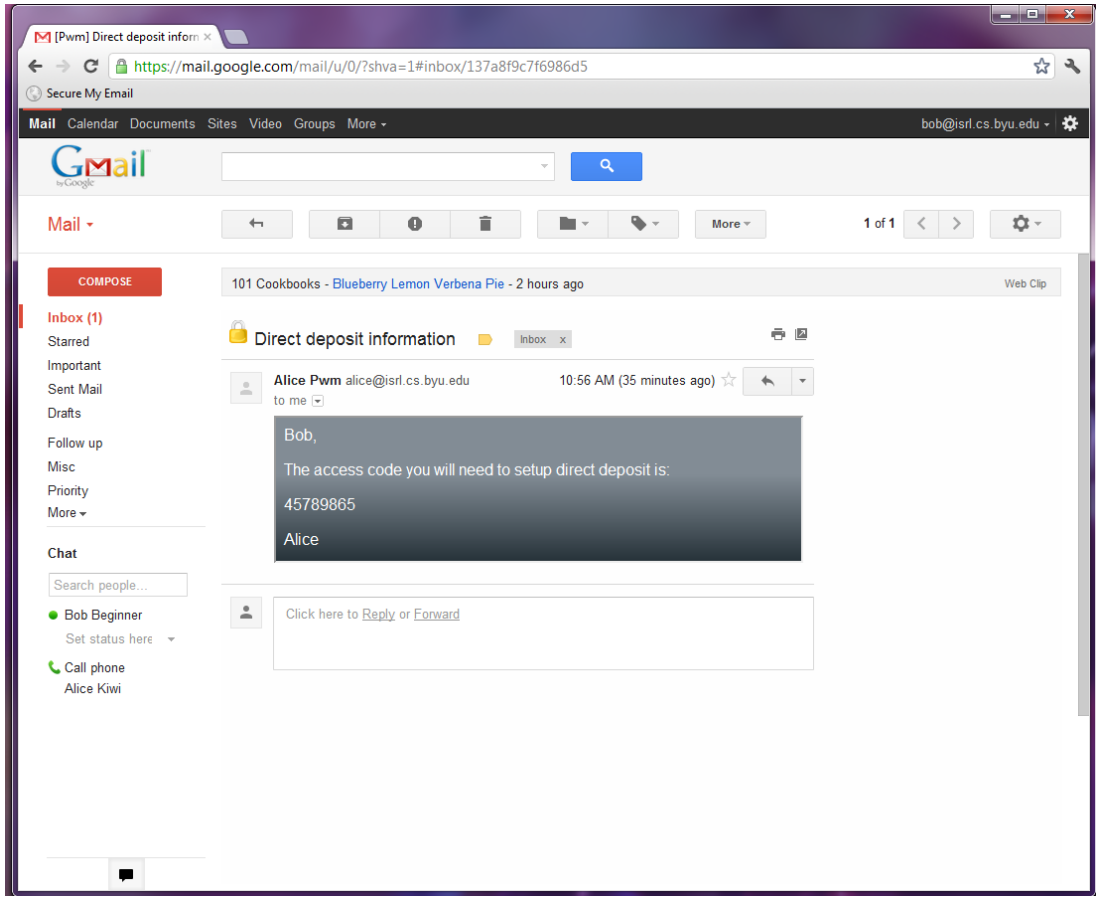
\+ Autenticazione invisibile ed automatizzata.

Dettagli tecnici Pwm 1.0: cifratura automatica

- Decifra automaticamente.
- Risposta a messaggio cifrato automaticamente cifrata.
- Nuovi messaggi richiedono l'attivazione delle cifratura.

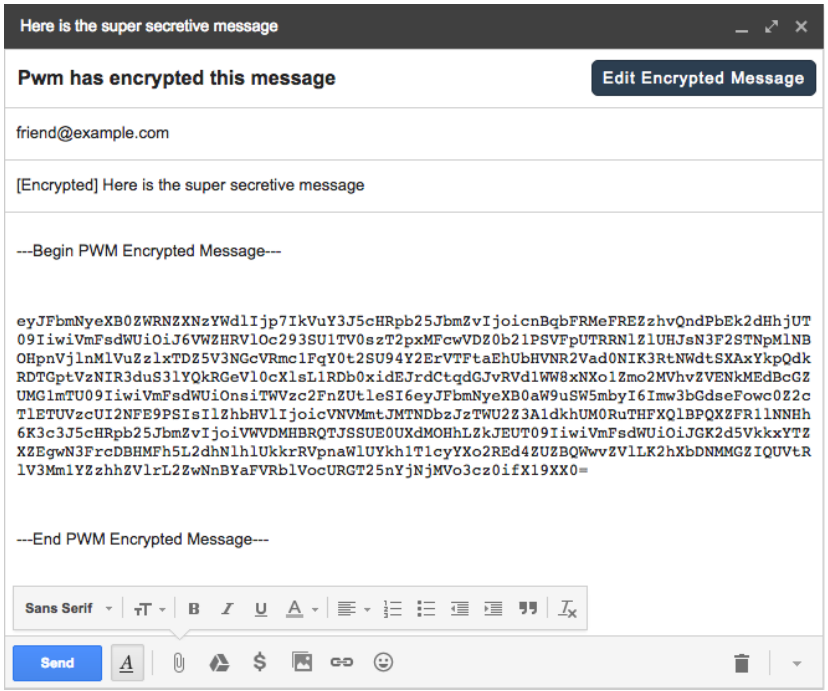
Limita il numero di utenti che devono installare Pwm.

Dettagli tecnici Pwm 1.0: cifratura automatica



Approfondimento di "Private Webmail (Pwm) 1.0".

Cifratura Automatica vs Manuale



Cifratura Manuale

1. Si preme "Encrypt" $\Rightarrow$ viene mostrato il cyphertext.
2. Si preme "Send".

Ottimi risultati in mockup test.

Cifratura Automatica vs Manuale

Due versione di Pwm 2.0:

- Pwm 2.0 cifratura automatica.
- Pwm 2.0 cifratura manuale.

Differenze di punteggio di usabilità non significative.

Approfondimento di "Miglioramento di Usabilità: Cifratura Ritardata".

Scenari e Tasks nel dettaglio

Per ogni partecipante:

- Registrazione video.
- Se mail in chiaro, si segna un errore e ripete il task.
- Misurato il tempo di completamento di ogni task.

Scenario 1: essere assunti per un nuovo lavoro

1. Ricevuta mail con informazioni minimali sul set-up e con richiesta di dati sensibili. Set-up ed invio cifrando.
2. Decifrare una mail e replicare in CC.
3. Inoltrare una mail con informazioni sensibili cifrate.
4. Inviare dati sensibili cifrandoli (la cifratura non è sollecitata).

Scenari e Tasks nel dettaglio

Per ogni partecipante:

- Registrazione video.
- Se mail in chiaro, si segna un errore e ripete il task.
- Misurato il tempo di completamento di ogni task.

Scenario 2: inviare dati sensibili al proprio compagno/a

1. Istruire una persona all'utilizzo di Pwm e inviarle dati sensibili cifrati.
2. Inviare dati sensibili cifrandoli (la cifratura non è sollecitata).

Struttura dello user-study

1. Introduzione allo studio e questionario demografico.
2. Tasks.
3. Questionario sull'esperienza.
4. Questionario proprietà crittografiche.
5. Intervista post studio.

Qualtrics web-based survey sw per la gestione dei questionari.

SUS Questions

Choose from 1 (strongly disagree) to 5 (strongly agree).

1. I think that I would like to use this system frequently
2. I found the system unnecessarily complex
3. I thought the system was easy to use
4. I think that I would need the support of a technical person to be able to use this system
5. I found the various functions in this system were well integrated
6. I thought there was too much inconsistency in this system
7. I found the system very cumbersome to use
8. I would imagine that most people would learn to use this system very quickly
9. I felt very confident using the system
10. I needed to learn a lot of things before I could get going with this system

Threat Model

- Webmail provider: Honest-but-Curious, accede ai messaggi cifrati.
- Key server: Honest-but-Curious, accede alle chiavi private.
- Attaccante: monitora ogni comunicazione, intercetta pacchetti cifrati.

Per ottenere i dati sensibili, è necessario:

1. ottenere la mail cifrata.
   - compromettendo il webmail provider.
   - intercettando una mail non trasmessa usando TLS.
2. ottenere la chiave per decifrarla.
   - compromettendo il key server.