Understanding User Tradeoffs for Search in Encrypted Communication

Wei Bai, Ciara Lynton, Charalampos (Babis) Papamanthou, Michelle L. Mazurek
Contacts: {wbai, clynton, cpap, mmazurek}@umd.edu
University of Maryland, College Park
USENIX SOUPS 2018

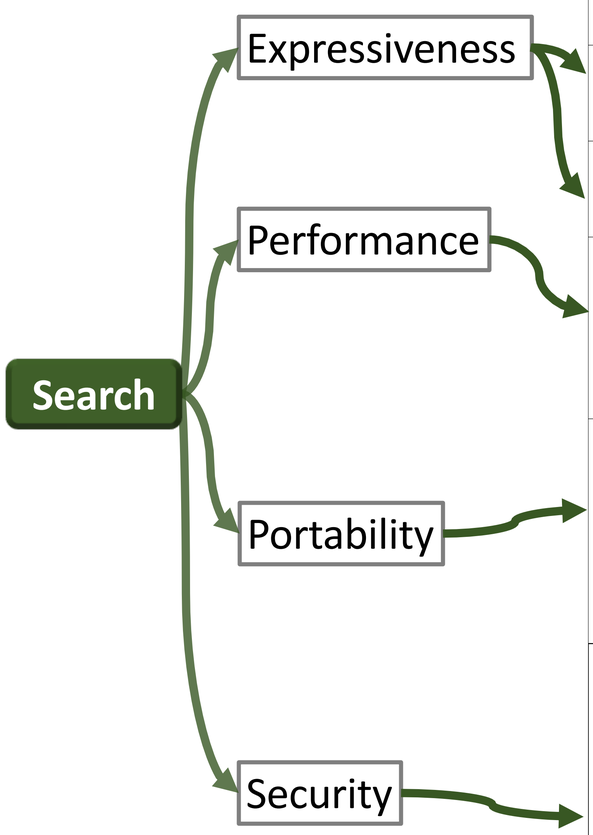
Motivation

- End-to-end message encryption provides strong privacy
- Searching encrypted messages is complicated
- *Local search*: store a search index locally on the device
- *Searchable encryption*: search encrypted messages directly

How do general users trade off usability and security?

Searchable Encryption

Study Design



Feature	Options
Price	**$0.00 (free)** or $**1.99 per month**
Multi-word Email Search	**Yes** or **No**
Partial-word Email Search	**Yes** or **No**
Storage on your device	**Will use 5MB on your device, equivalent to about 2-3 HD photos** or **Will use 500MB on your device, equivalent to about 200 HD photos or 20 mobile apps**
Syncing old email to a new device	**Yes – read and search all email using the new device** both before and after its activation. **No – read and search only email after you configured the new device**. You can't read and search old emails on your new device.
Privacy	**Standard privacy**: Your email service can access the contents of all email and email search queries. **Extra privacy**: Your email service can access the contents of certain emails and email search queries, but not all. **Maximum privacy**: Your email service cannot access the contents of any emails or email search queries.

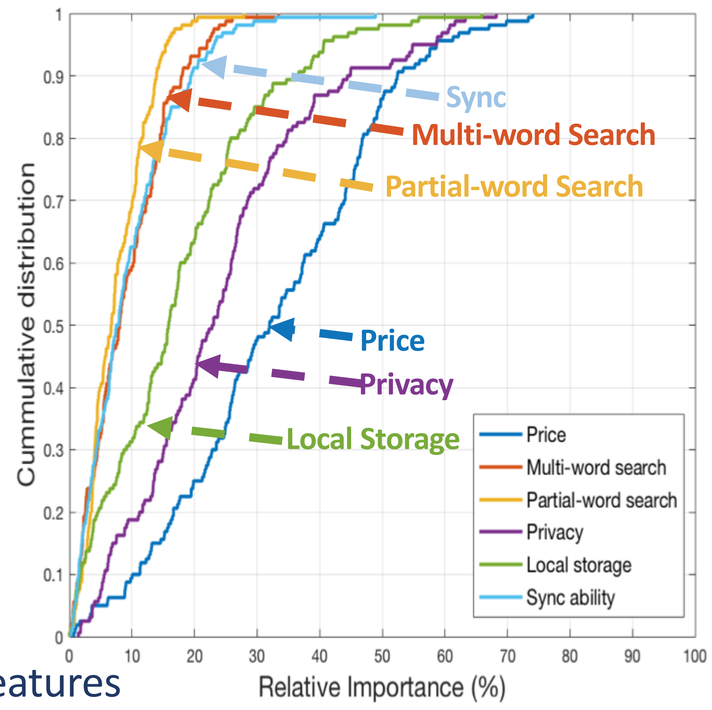
User Study: Conjoint Analysis (16 questions)

	Email Service 1	Email Service 2
Price	$0.00 (free)	$0.00 (free)
Multi-word Email Search	No	No
Partial-word Email Search	Yes	No
Privacy	Extra privacy-–email service can access some emails and email search queries	Maximum privacy—email service cannot access any emails or email search queries
Storage on your device	Will use 5MB on your device, equivalent to about 2-3 HD photos	Will use 5 MB on your device, equivalent to about 2-3 HD photos
Syncing old emails to a new device	Yes—read and search all email using the new device	No—read and search only email after you configured the new device

Question: If you were considering recommending a personal, non-work email service to your friends, and these were the only alternatives, which would you recommend?

Value of Features & Options

Features	Option Change	Dollar Value	Relative Importance
Price	$1.99 -> $0.00		32.59%
Privacy	Standard -> Extra	$0.86	24.19%
	Extra -> Maximum	$0.55	
	Standard -> Maximum	$1.41	
Local Storage	500 MB -> 5MB	$0.68	17.38%
Sync Ability	No -> Yes	$0.44	9.36%
Multi-word Search	No -> Yes	$0.49	9.02%
Partial-word Search	No -> Yes	$0.42	7.46%



- Privacy and local storage: most valued non-monetary features
- Marginal benefit of privacy: decreases
- Less local storage requirement ≈ Privacy improvements
- Advanced search and sync abilities: less valued
- Variations: important features > less important features

Conclusions

In the email context:

- Local indexing search will likely work for many users
- There may be a niche for searchable encryption
  - Some users: worthwhile, increased privacy and not too much required storage
  - Designers: focus on privacy and convenience
- No "one-size-fits-all" solution
  - Designers: may design a switch for local/cloud indexing search

Reference: Understanding User Tradeoffs for Search in Encrypted Communication. IEEE European Symposium on Security and Privacy (EuroS&P). London, United Kingdom. April 2018.