UiO : University of Oslo

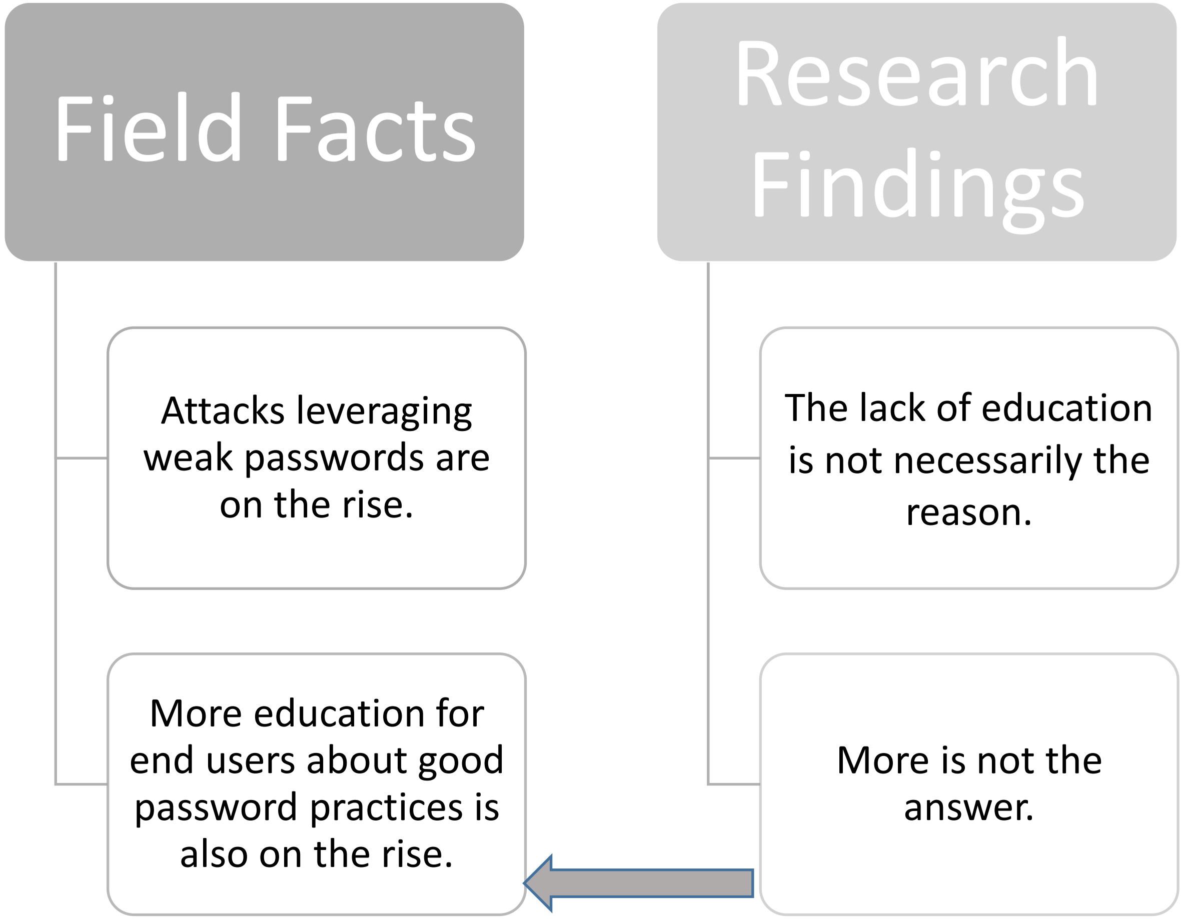
Passwords are not always stronger on the other side of the fence

Ijlal Loutfi, Audun Jøsang
University of Oslo
Mathematics and Natural Sciences Faculty

USEC 2015, San Diego, USA
February, 8th 2015

The Backstory

What we found out



Field Facts

Attacks leveraging weak passwords are on the rise.

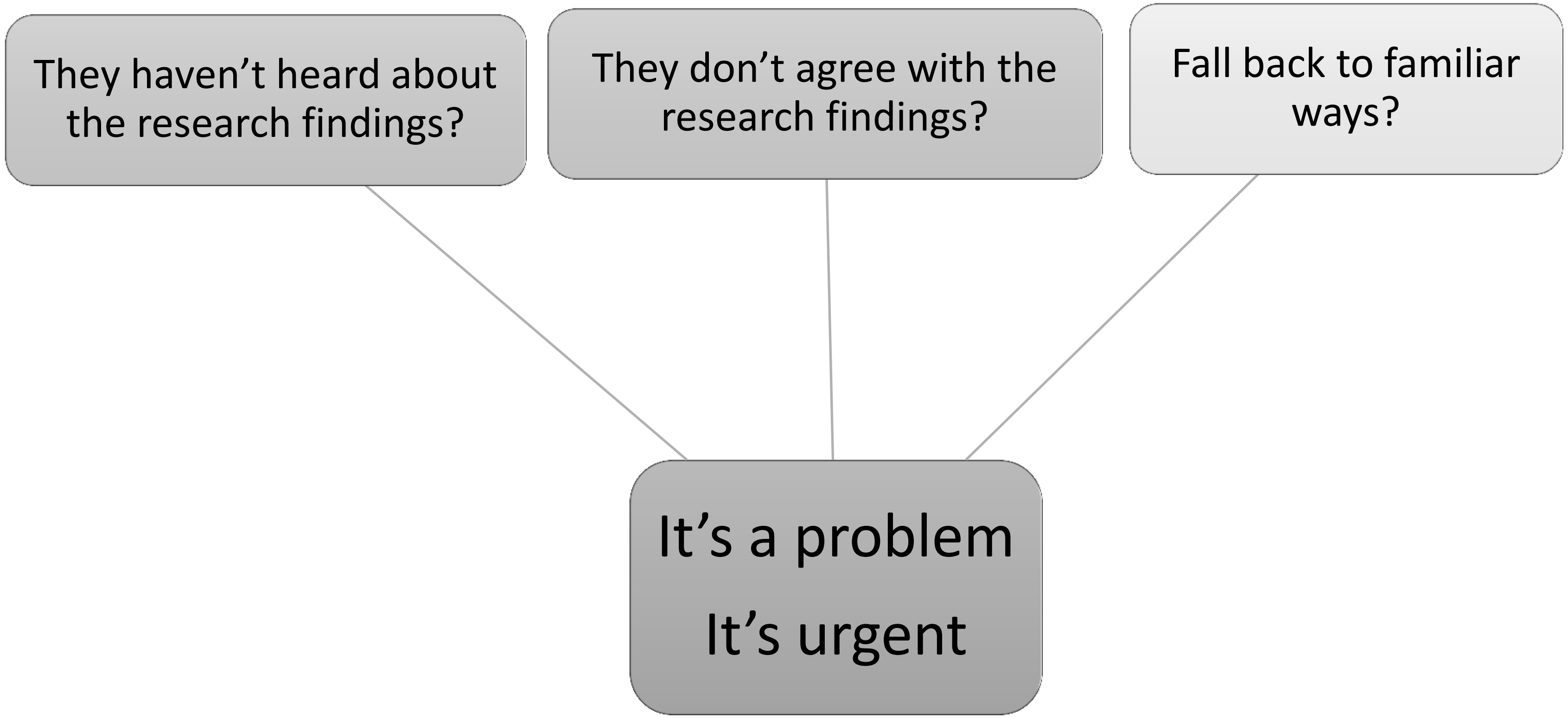
More education for end users about good password practices is also on the rise.

Research Findings

The lack of education is not necessarily the reason.

More is not the answer.

The Gap



They haven’t heard about the research findings?

They don’t agree with the research findings?

Fall back to familiar ways?

It’s a problem

It’s urgent

The Gap

IT Professionals

are an important part of the equation

What to do about it?

Hold up a mirror

- Straightforward
- Explicit
- Calls for involvment
- Simple

- Survey
- Audience: IT Professionals.

Formulating the Hypothesis

Education is a necessary yet not by itself a satisfactory condition for ensuring safe password behaviors?

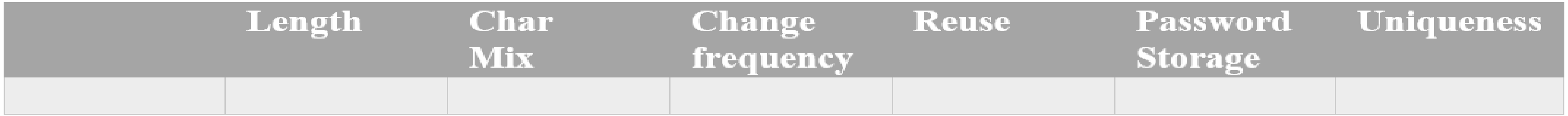
Cognitive knowledge does not always materialize into practical behavior?

What was measured?

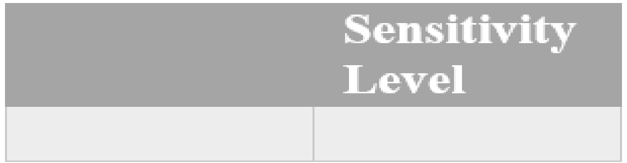
- Independent variables: Gender, Age, Educational Level, Sector of activity.
- 8 services: Facebook, Gmail, LinkedIn, Twitter, Work/studies email, bank account, online gaming accounts and online storage services.

- Reported sensitivity level: Level of sensitivity a user judges a service to be to them.
- Reported password behavior: Measure induced from the individual answers the users provide about specific aspects of the password they use for each service (e.g.: length, character mix...etc.)
- Perceived password behavior: Judgment the users hold about how healthy their password behavior is.

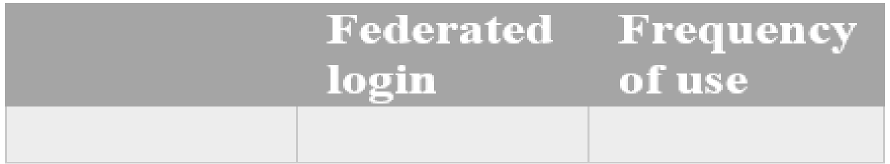
How was is measured?



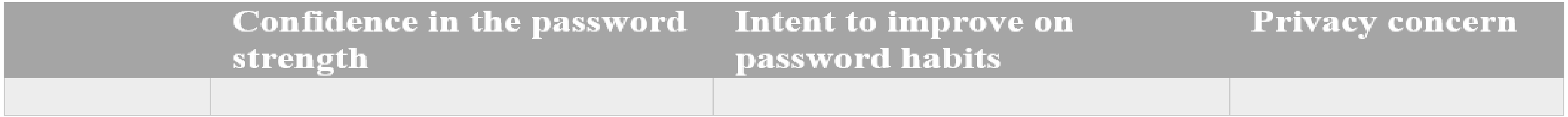
	Length	Char Mix	Change frequency	Reuse	Password Storage	Uniqueness



	Sensitivity Level



	Federated login	Frequency of use



	Confidence in the password strength	Intent to improve on password habits	Privacy concern

Survey considerations

Questions placement:

- Password habits
- Sensitivity level

- Confidence level in the passwords’ strength
- Intent to improve password behavior

- Federated login usage
- Privacy concern

Analysis

- 1st iteration :
  - Data at its most granular level

- 2nd iteration:
  - Correlations:
    - Service
    - Respondent
    - Behavior

Analysis methods

- Chi square test.

- Chi square test performed against the null hypothesis.
  - Two categorical variables are completely independent.
  - Significance value: 0.05
  - Data visualization

- Residual deviation of each pair
  - Significance range: (-2,2)

Findings: 1st iteration-Reported behaviors

- Hacking attacks don’t discriminate: 26 percent
- Storage habits: 11 percent store them in the clear
- Character mix
  - Worst behavior exhibited regarding Facebook and LinkedIn
  - Average 30 percent
- Password change frequency: Rarely or when asked
- Password uniqueness: Reused (42, 60) - Work/Studies
- Password length: over 6 (97)

Findings: 1st iteration

- Confidence: 17%, 55%, 18%, 8%, 3%.

- Privacy Concern.

Findings: 2nd Iteration

- Focus on services.

- Sensitivity level vs. reported password behavior:
  - Strongest correlation: Password length (high sensitivity, increased password length).
  - Character mix.
  - Insignificant correlations for the rest of the features.

Findings: 2nd Iteration

- Focus on behavior:
  - Define a safe password behavior profile.

✓ 12% of passwords satisfy the safe password behavior profile!

- Focus on the respondents:
  - ✓ 50% of the passwords mapped to 30 % of the respondents that are part of the above subset.
  - ✓100% respondents: Level 3 confidence
  - ✓75%: Intent to improve password behavior
- No correlation between the expressed privacy concern and the usage of federated login

Conclusions and Lessons Learned

- IT professionals possess the needed cognitive knowledge about password behaviors.
- Password behaviors reported are NOT good enough.

- Sensitivity level does not correlate with all the features needed for a safe password behavior
  - The ever more granular advice?

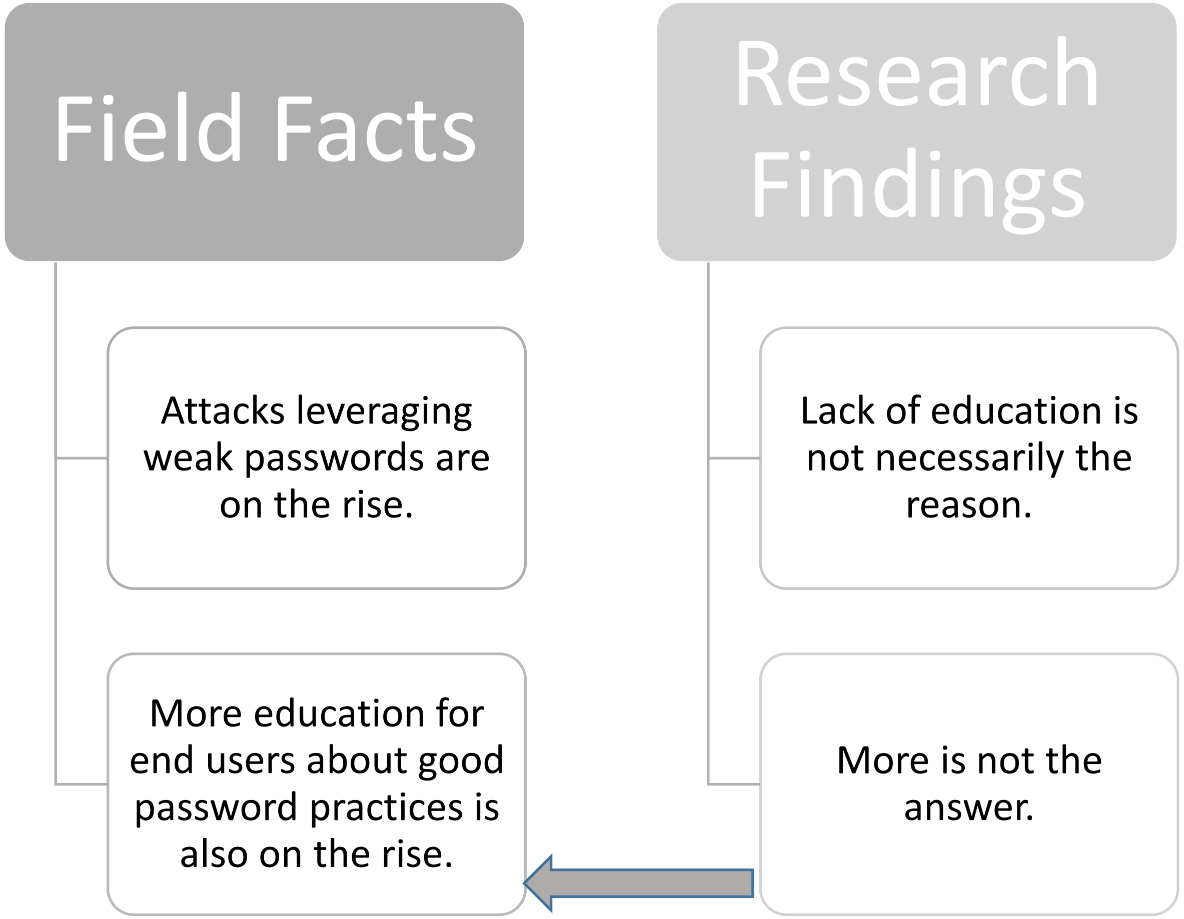
- ROI?

Hypothesis?

Education is a necessary yet not by itself a satisfactory condition for ensuring a safe password behavior.

Cognitive knowledge does not always materialize into practical behavior.

Closing the Gap?



Field Facts

Attacks leveraging weak passwords are on the rise.

More education for end users about good password practices is also on the rise.

Research Findings

Lack of education is not necessarily the reason.

More is not the answer.

Lessons Learned

- IT professionals can play a vital role in shifting perceptions about security in general:
  - Solutions
  - Sensitivity of the roles they hold
- Research findings ought to speak to the concerned people directly and involve them.

Acknowledgements

- The respondents for their time.
- Thanks to the USEC 2015 anonymous reviewers, as well as our shepherd, Dr. Jens Grossklags.
- COINS Research School of Computer and Information Security.

Thank you.