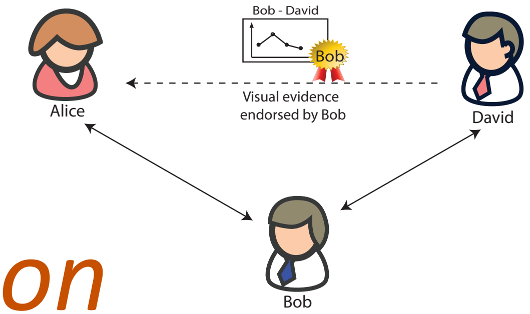
RelationGram:

Tie-Strength Visualization for User-Controlled Online Identity Authentication



Tiffany Hyun-Jin Kim, Virgil Gligor, Jason Hong, Adrian Perrig

Carnegie Mellon University

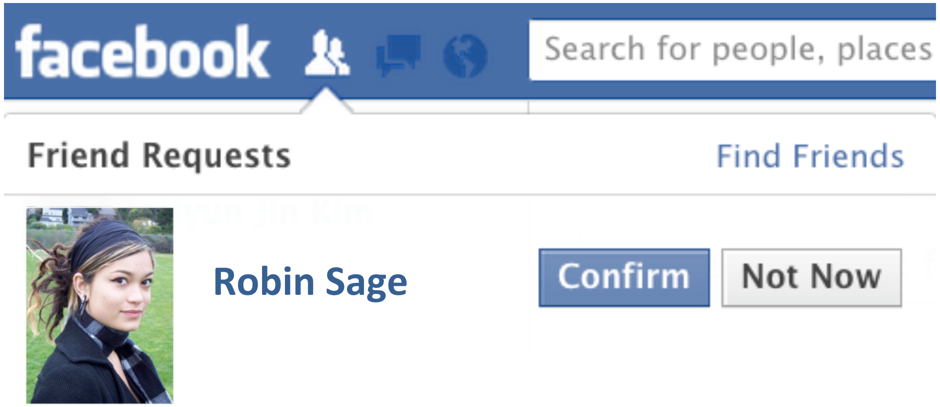
Akira Yamada

KDDI R&D Laboratories

Financial Cryptography and Data Security 2013

April 2, 2013

ONLINE INVITATIONS

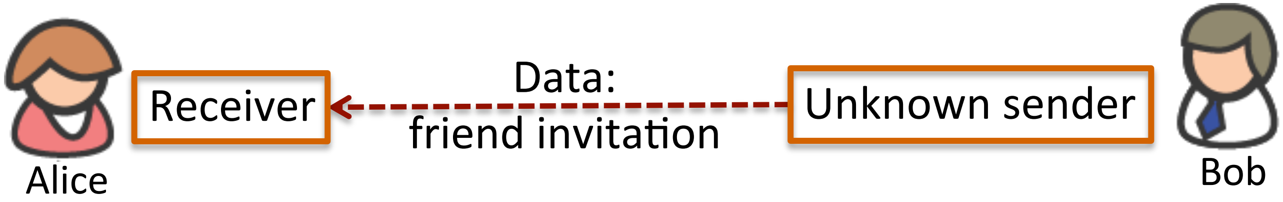


- **Is this request from claimed sender?**
  - Easy to create bogus identity
  - For both non-existing and existing people
    - Phony female: Robin Sage – fooled security-savvy users[1]
    - Existing people – Sensitive info available online

[1] T. Ryan. Getting in Bed with Robin Sage. In *Proceedings of the Black Hat Conference*, 2010

DATA ASYMMETRY

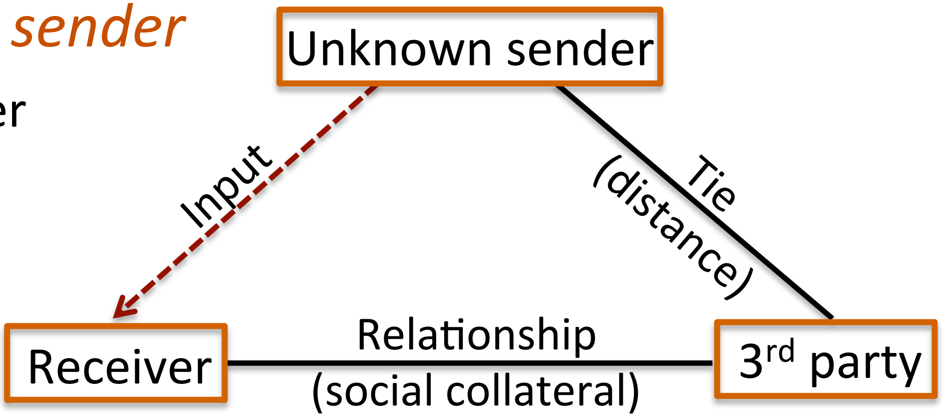
- **Fundamental problem**
  - Sender knows *more* about sent data than receiver



- **How can we reduce asymmetry such that receiver (user) can achieve authentication trust for data?**

HOW TO REDUCE ASYMMETRY

- **Delegate trust decision to 3rd party**
  - 3rd party has relationship with *receiver*
    - Misbehavior to receiver ➔ loss of social collateral
  - 3rd party knows *unknown sender*
    - No need to trust each other

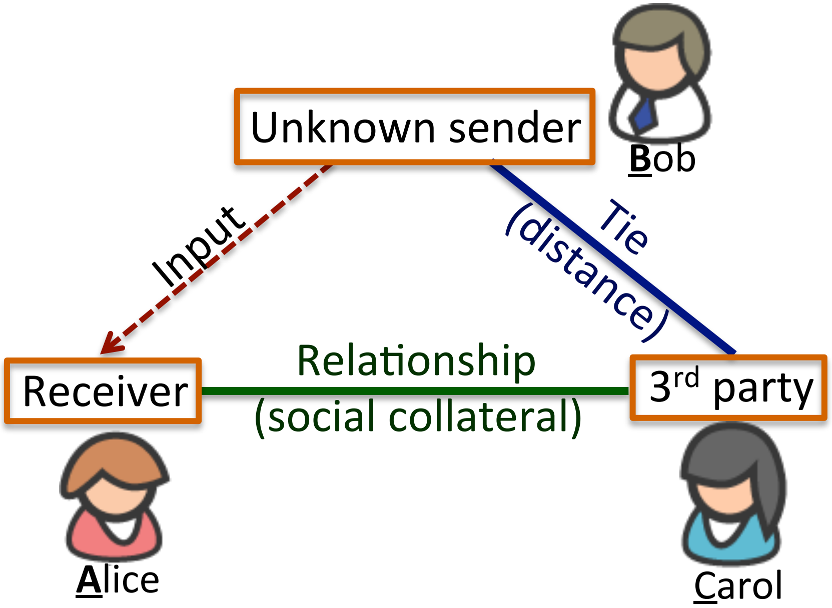


  - *Recommends* unknown sender to receiver

WHEN WILL RECEIVER ACCEPT INPUT?

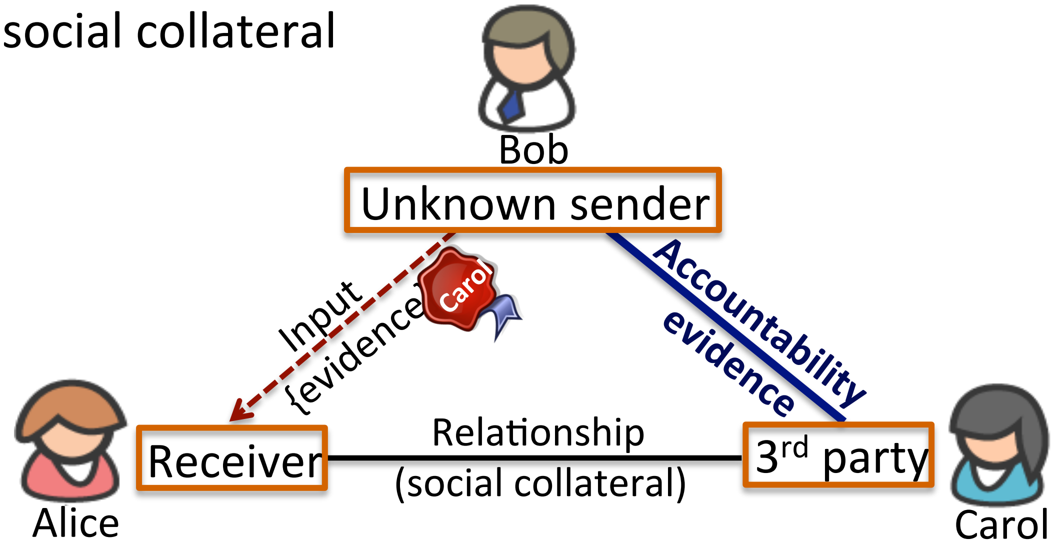
Notation	Meaning
SC(C)@A	Social collateral that C has with A
SC(B)@C	Social collateral *assigned by A* that B has with C

- **Acceptability**
  - $SC(B)@C \geq T_A(app, attr)$
- **Deterrence**
  - $SC(C)@A - SC(B)@C \geq P_A(app, attr)$



SOCIAL COLLATERAL MODEL[2]

- **Accountability evidence**
  - "Carol is accountable for providing correct evidence about her knowledge about Bob to Alice"
  - Bob forwards accountability evidence endorsed by Carol
  - Carol is *deterred* from providing false evidence to Alice
    - i.e., loss of social collateral

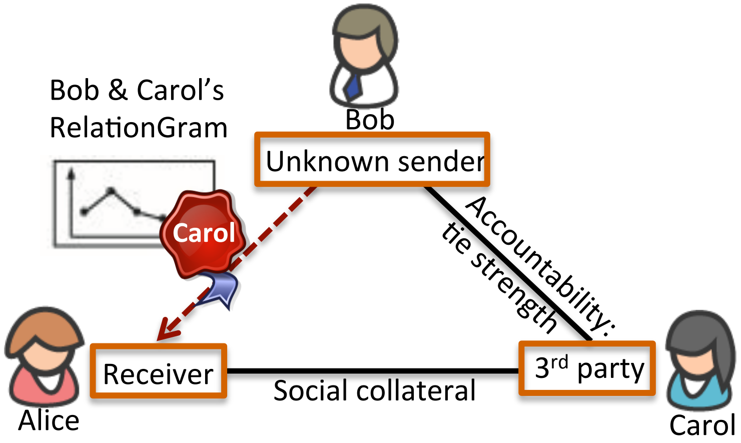


[2] T. H.-J. Kim, V. Gligor, and A. Perrig. Street-Level Trust Semantics for Attribute Authentiation. In *Security Protocols Workshop*, 2012.

RelationGram

- **Useful accountability evidence indicator: tie strength[3]**
  - Closeness or social proximity of two individuals
    - Strong tie: people you really trust
    - Weak tie: loose acquaintances

- **Tie strength visualization[4]**
  - Meaningful and intuitive
  - With different combinations of parameters



- **Why visualization?**
  - Simple numbers may not capture tie strength *with sufficient granularity*
    - Context-dependent nature of trust
  - Instead, we provide *evidence* and let people decide

[3] M. Granovetter. The Strength of Weak Ties: A Network Theory Revisited. *Sociological Theory*, 1, 201-233. 1983.
[4] T. H.-J. Kim, V. Gligor, J. Guajardo, J. Hong, and A. Perrig. Soulmate or Acquaintance? Visualizing Tie Strength for Trust Inference. In *USEC 2013*.

DESIRED PROPERTIES

- **Meaningful**
  - Diagram should convey *meaningful & useful tie strength info*
- **Intuitive**
  - Users can understand diagram *without difficulties*
- **Robust**
  - Diagram is robust against attackers *manipulating tie strength*

- **Adversary goal: make victims accept invitations**
  - Manipulate social parameters
  - Gather sensitive info of victims & their friends
- **Do not consider account compromise**

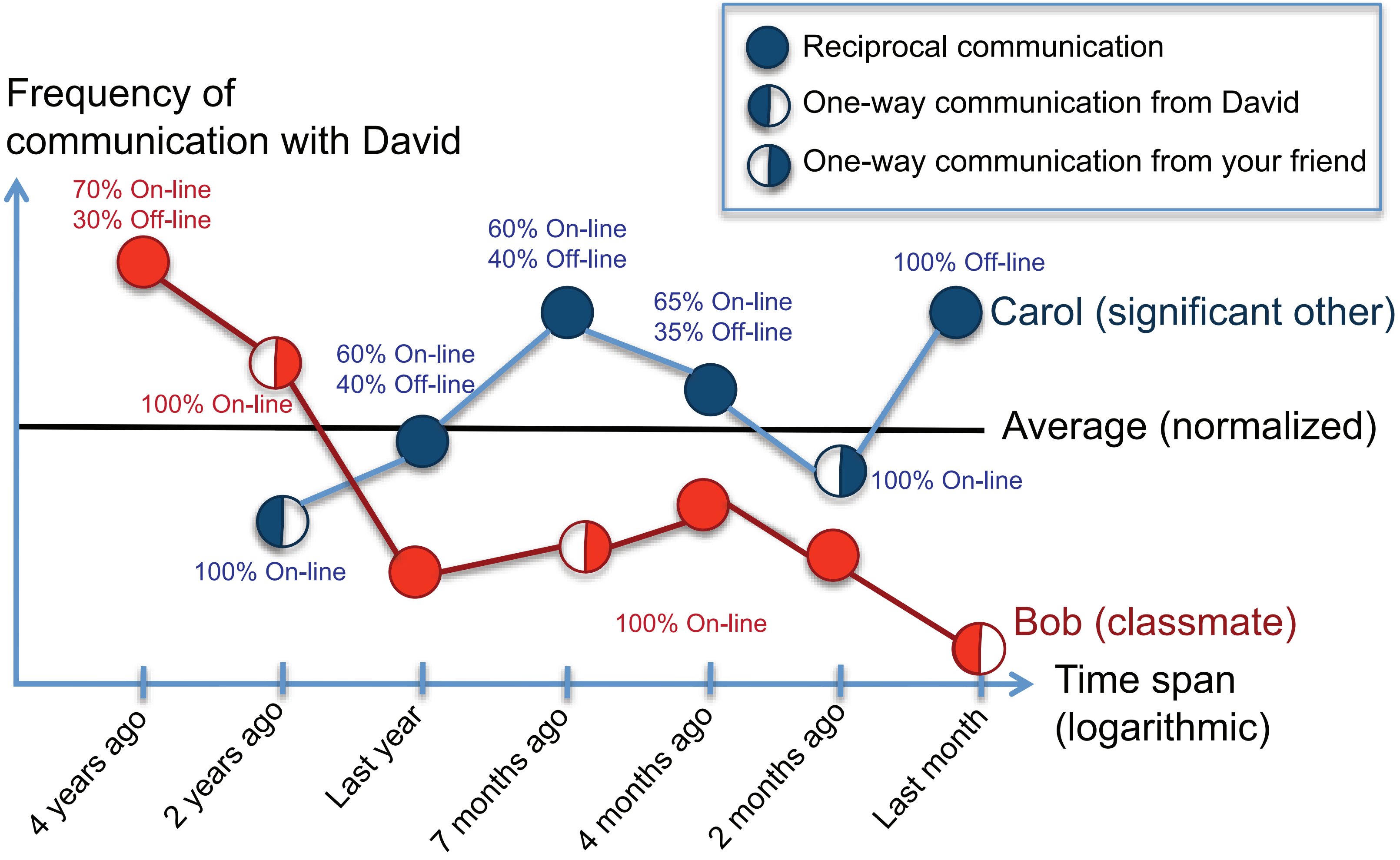
RELEVANT PARAMETERS

- **Intensity**
  - Amount of time spent
  - Phone calls/emails exchanged
  - Frequency of interaction[5]
- **Intimacy**
  - Days since last communication
  - Distance between hometowns
  - Appearances in photos
- **Reciprocal services**
  - Applications in common
  - Communication reciprocity[5]
- **Duration**
  - Length of relationship[6]
- **Structural**
  - Network topology
  - Mutual friends[5]
- **Emotional support**
  - Advice on family problems
- **Recency of interaction**[5]
- **Social distance**
  - Education level
  - Socioeconomic status
  - Political affiliation
  - Race, gencer, …

[5] E. Gilbert and K. Karahalios. Predicting Tie Strength With Social Media. In *CHI* 2010.

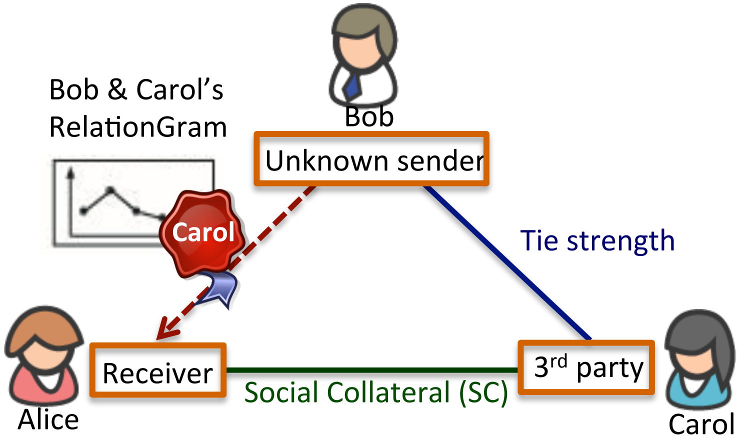
[6] B. Shneiderman. Designing Trust into Online Experiences. *Communications of the ACM*,43(12):57–59,2000.

RelationGram ILLUSTRATION



FRIEND AUTHENTICATION PROTOCOL

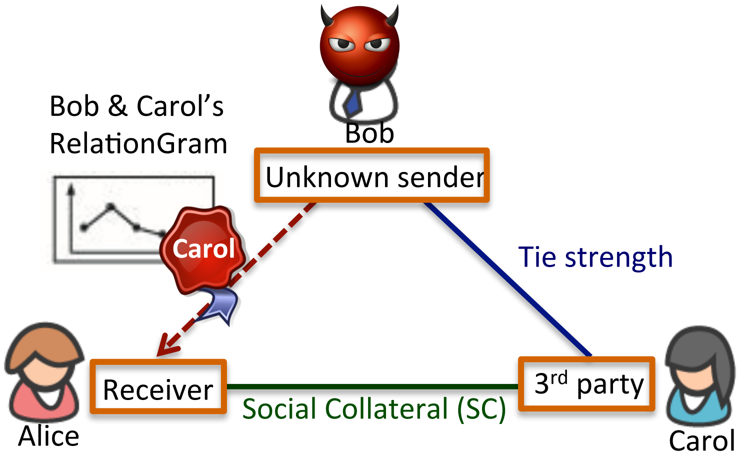
- **Evidence Generation**
  - Bob & Carol *mutually* agree to disclose graph to Alice
  - Carol's phone gathers tie strength info
    - Meeting, call history, SMS texts, Facebook posts, etc.
  - Carol signs RelationGram



- **Evidence Verification**
  - Alice checks Carol's signature
  - Alice authenticates Bob if
    1. Tie(Bob,Carol) ≥ Th_{Alice}
    2. SC(Alice,Carol) > Tie(Bob,Carol)
  - If 1 fails, Alice can request Bob to provide RelationGram from her *other* mutual friend

SECURITY ANALYSIS

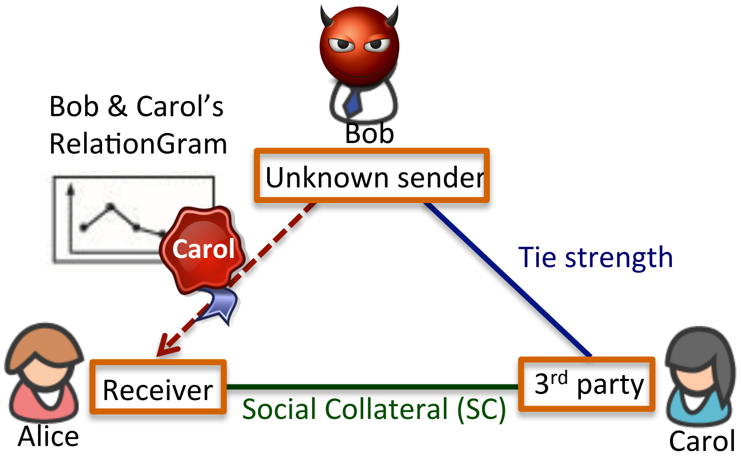
- **Inflation attack**
  - Each parameter (e.g., comm. frequency) can be inflated
  - *Combination* of multiple parameters → challenging

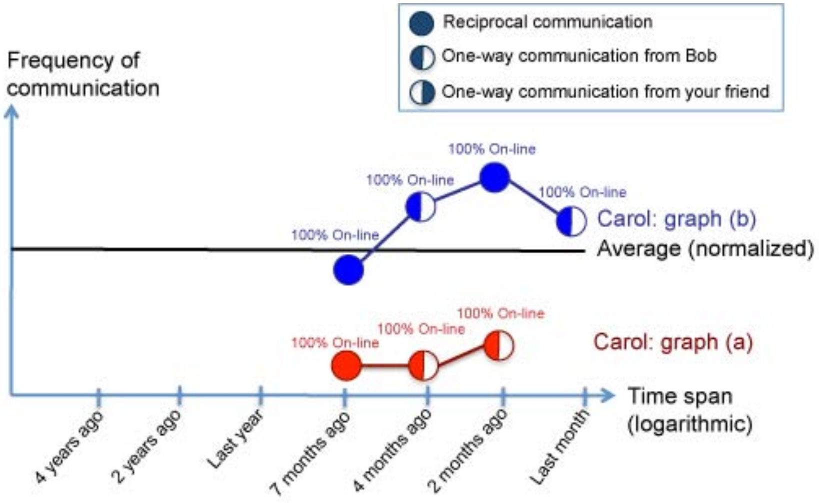


- **Collusion attack**
  - Bob has no way of learning Th_{Alice}
  - Bob colluding with Alice's *other* friend is low

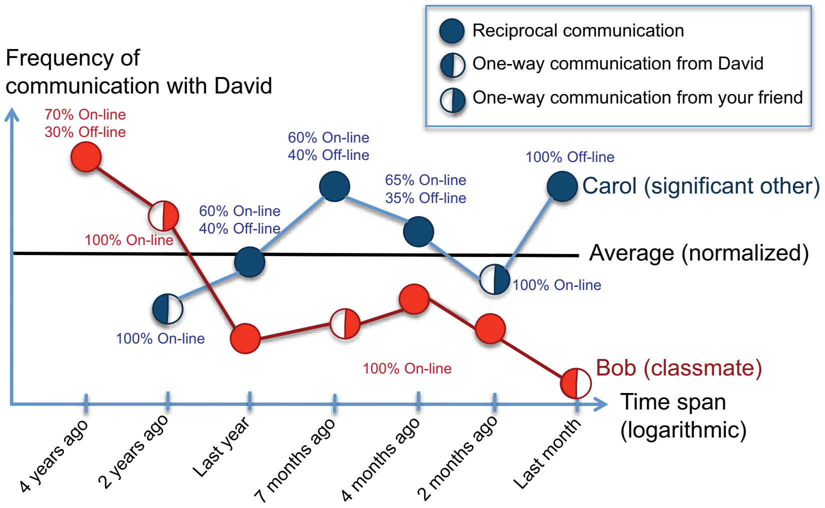
SECURITY ANALYSIS

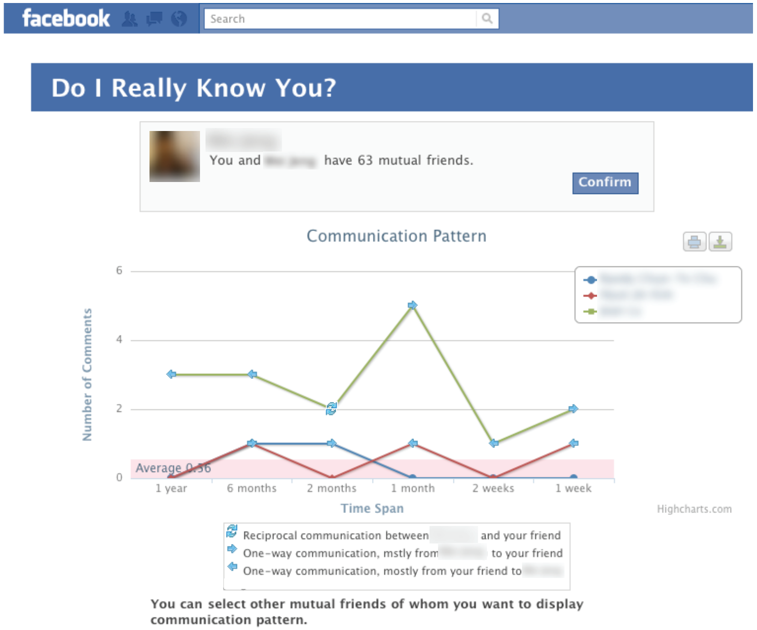
- **Impersonation attack**
  - Loss of social collateral deters Carol from endorsing Bob
  - *Unlikely* to have strong RelationGram





FACEBOOK APPLICATION





Do I Really Know You?

[redacted]
You and [redacted] have 63 mutual friends.

Confirm

Reciprocal communication between [redacted] and your friend
One-way communication, mstly from [redacted] to your friend
One-way communication, mostly from your friend to [redacted]

You can select other mutual friends of whom you want to display communication pattern.

- **User study**
  - Does RelationGram help users authenticate online inviters?
  - Amazon Mechanical Turk study
    - 100 participants → 93 eligible for analysis

RELATIONGRAM STUDY RESULTS

- **Relevance**
  - 85%: easy to understand tie strength of people on graphs
  - 85%: RelationGram captures tie strength

- **Robustness**
  - 90%: no strong tie → reject friend request

  → Can protect users from *potentially malicious strangers*

- **Privacy**
  - 82%: willing to share RelationGram with close friends and family

- **Usability**
  - 83%: RelationGram is easy to use
  - 88%: RelationGram is useful

CONCLUSIONS

- **RelationGram**
  - Improves identity authentication in virtual environments
  - Consistent with mental models from real-life experience
  - Enables users to safely authenticate online identities

- **People appreciate *situational awareness* gained from RelationGram**

- **Future work**
  - Trade-offs between burden on users vs. utility
  - Incentives for sharing RelationGrams