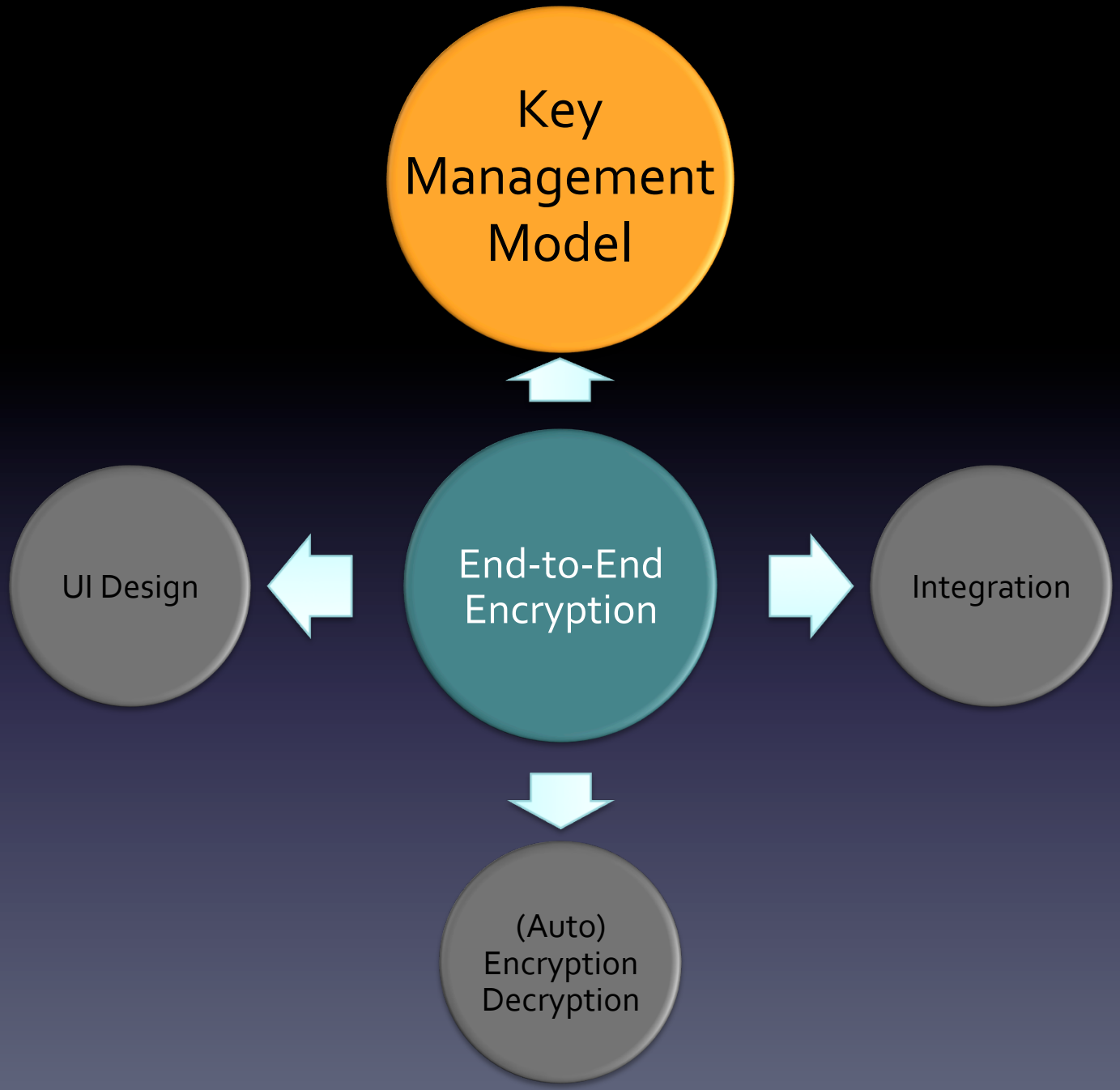
An Inconvenient Trust:

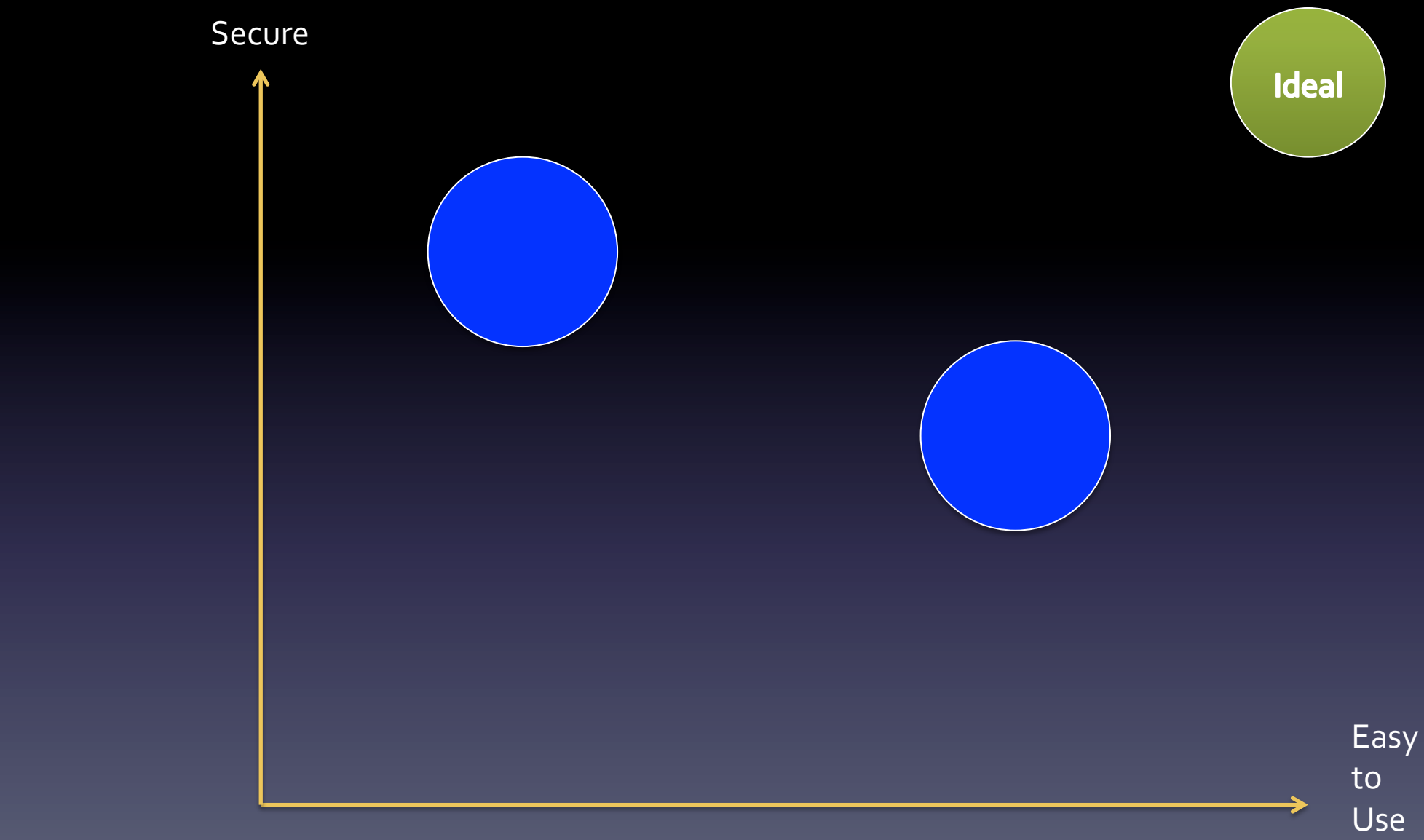
User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems

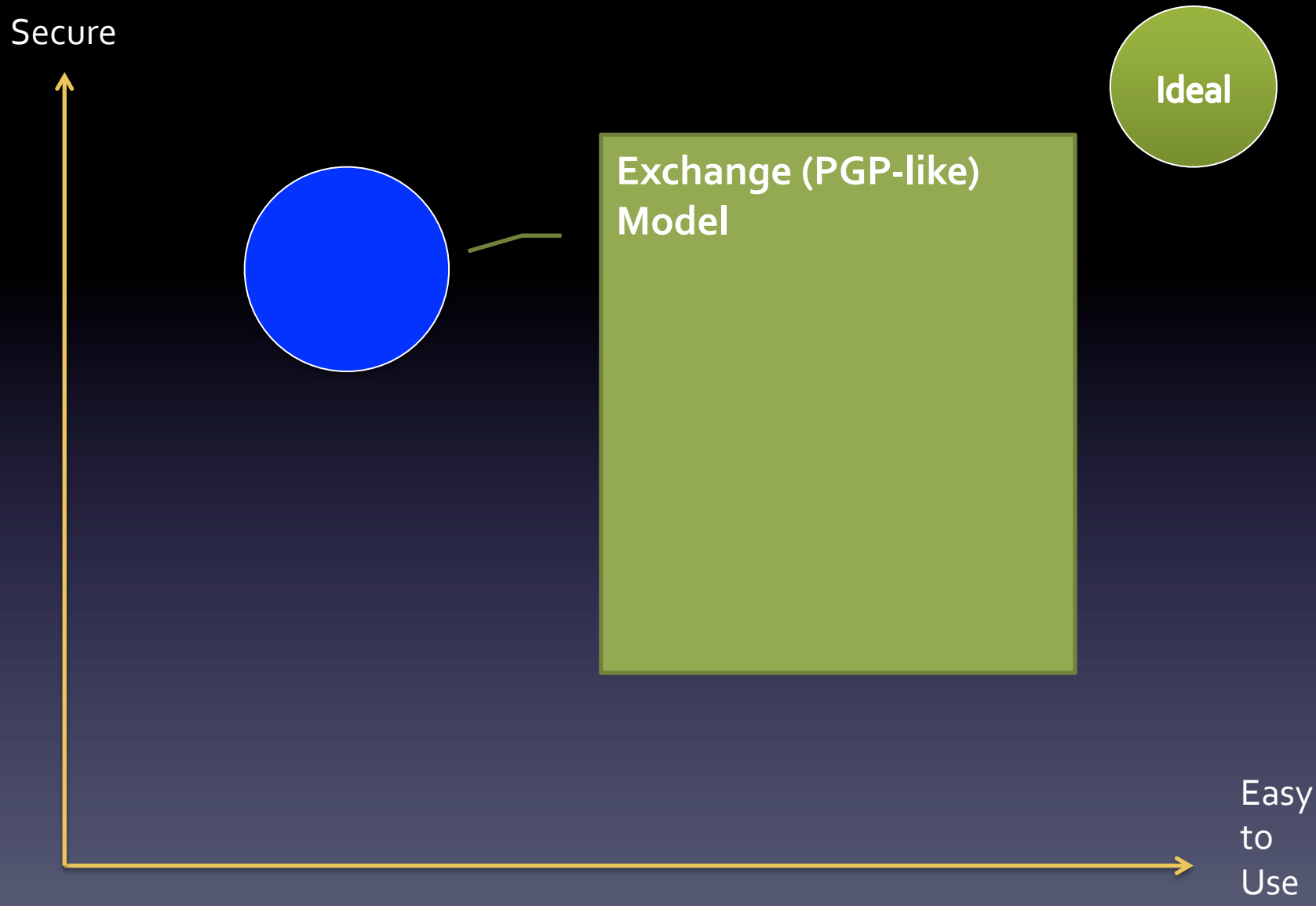
Wei Bai, Doowon Kim, Moses Namara, Yichen Qian,
Patrick Gage Kelley*, Michelle L. Mazurek
University of Maryland, College Park *University of New Mexico

What is End-to-End Encryption?

Hackers
Governments
Misbehaving Employees/Company Itself

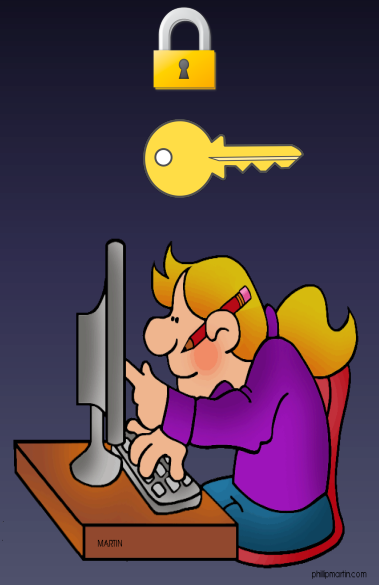

Key Management Model
End-to-End Encryption
UI Design
Integration
(Auto) Encryption Decryption


Secure
Ideal
Easy
to
Use

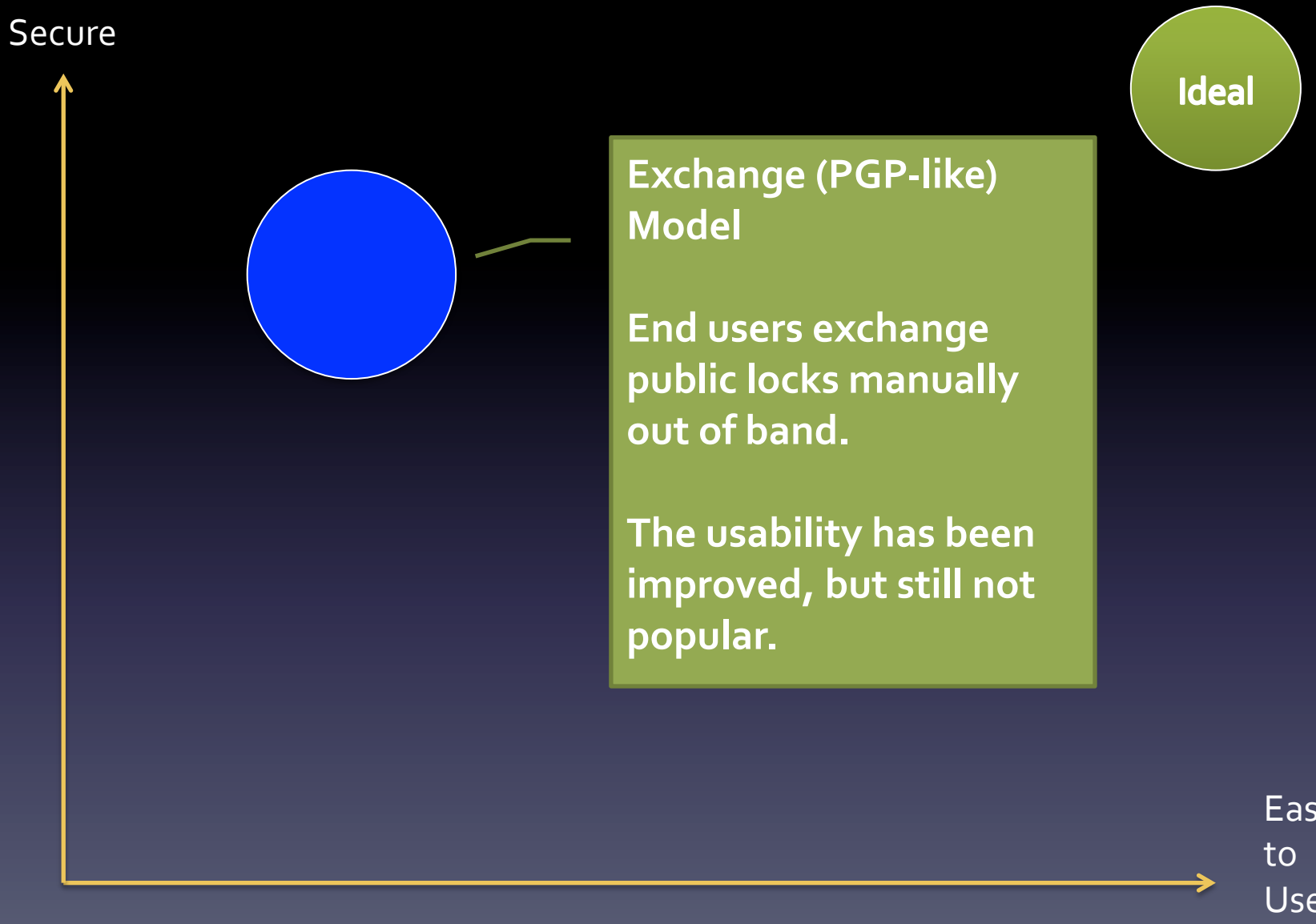

Secure
Ideal
Exchange (PGP-like) Model
Easy to Use

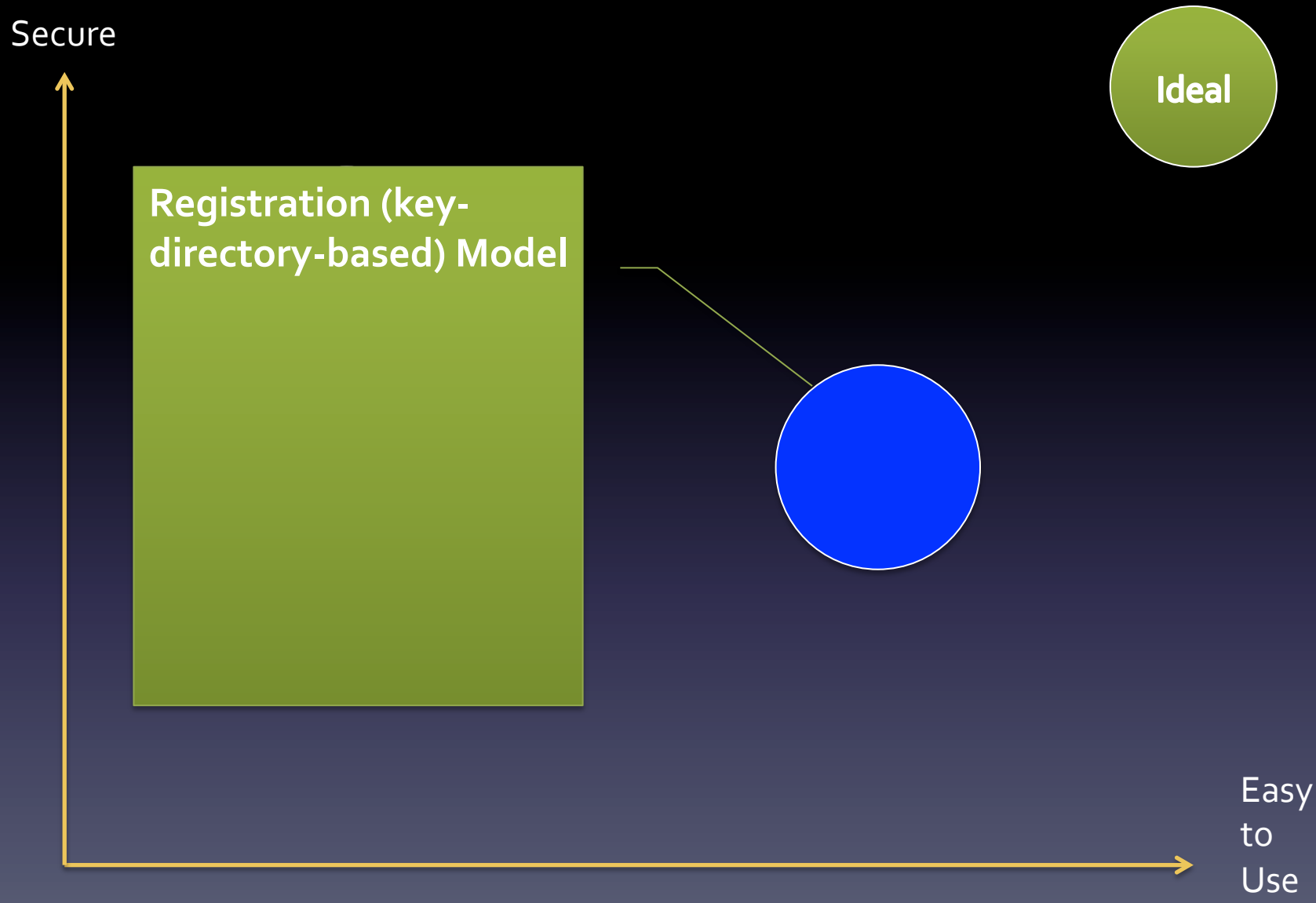
Exchange Model:

exchanging public locks[1] **manually out of band**

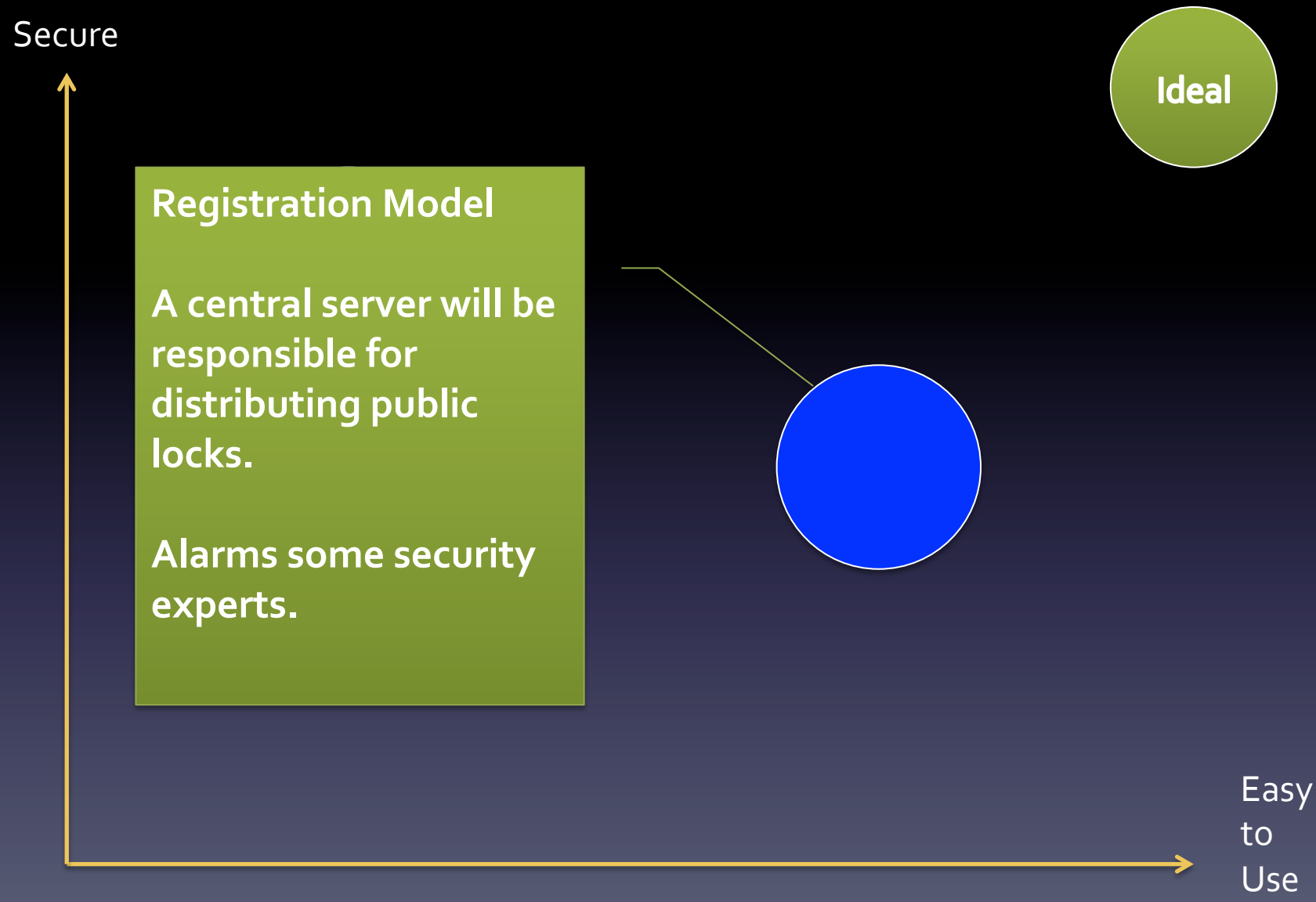


[1] W. Tong, S. Gold, S. Gichohi, M. Roman, and J. Frankle. Why King George III can encrypt. 2014


Secure
Ideal
Exchange (PGP-like) Model
End users exchange public locks manually out of band.
The usability has been improved, but still not popular.
Easy to Use

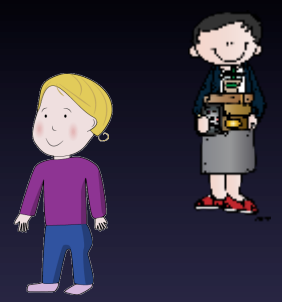

Secure
Ideal
Registration (key-directory-based) Model
Easy to Use

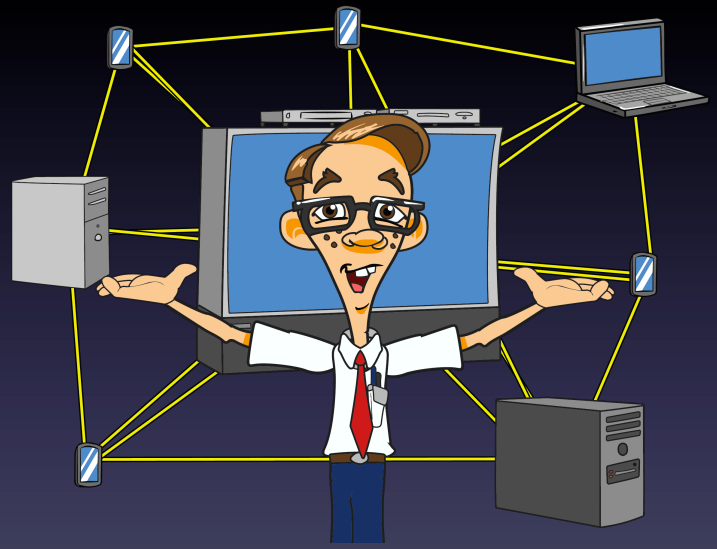
Registration Model


Secure
Ideal
Registration Model
A central server will be responsible for distributing public locks.
Alarms some security experts.
Easy to Use

Targeting General Users

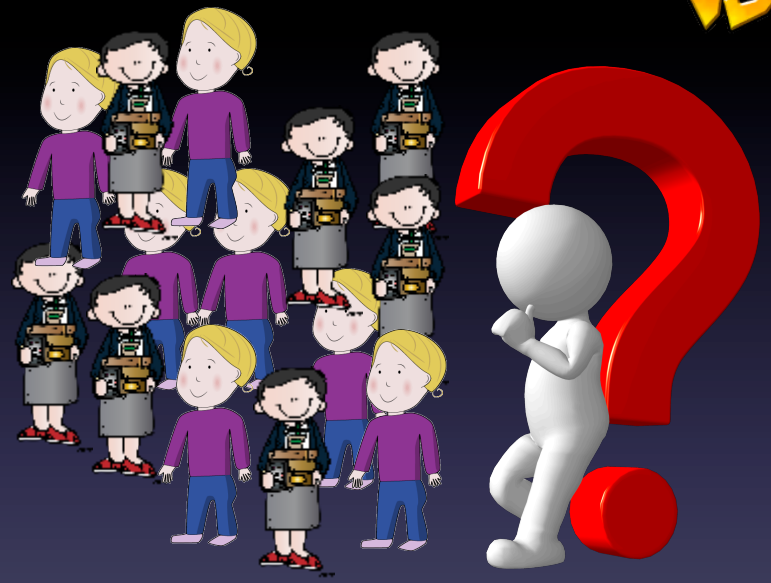
General Public VS Security Experts





Targeting General Users

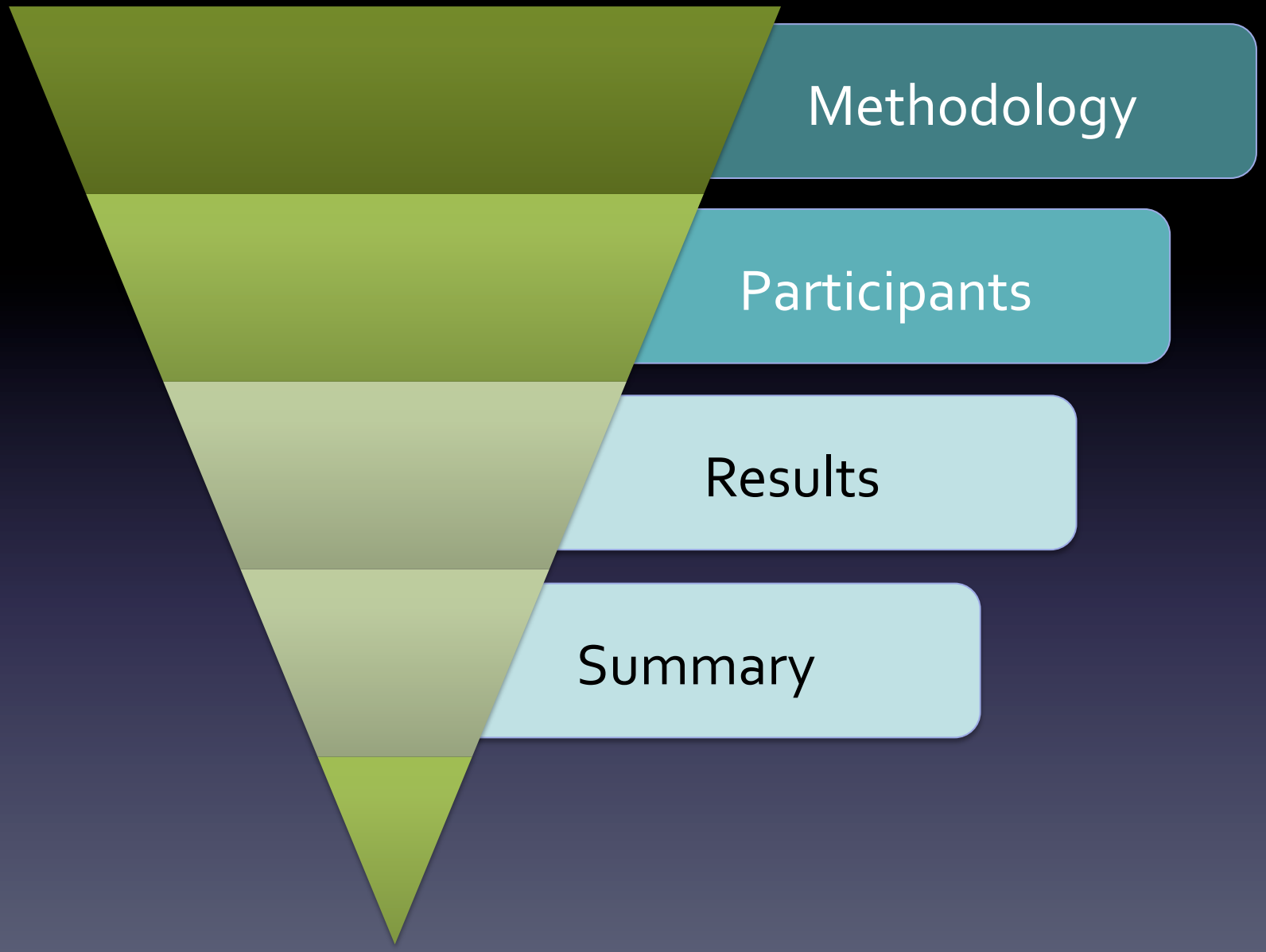
General Public

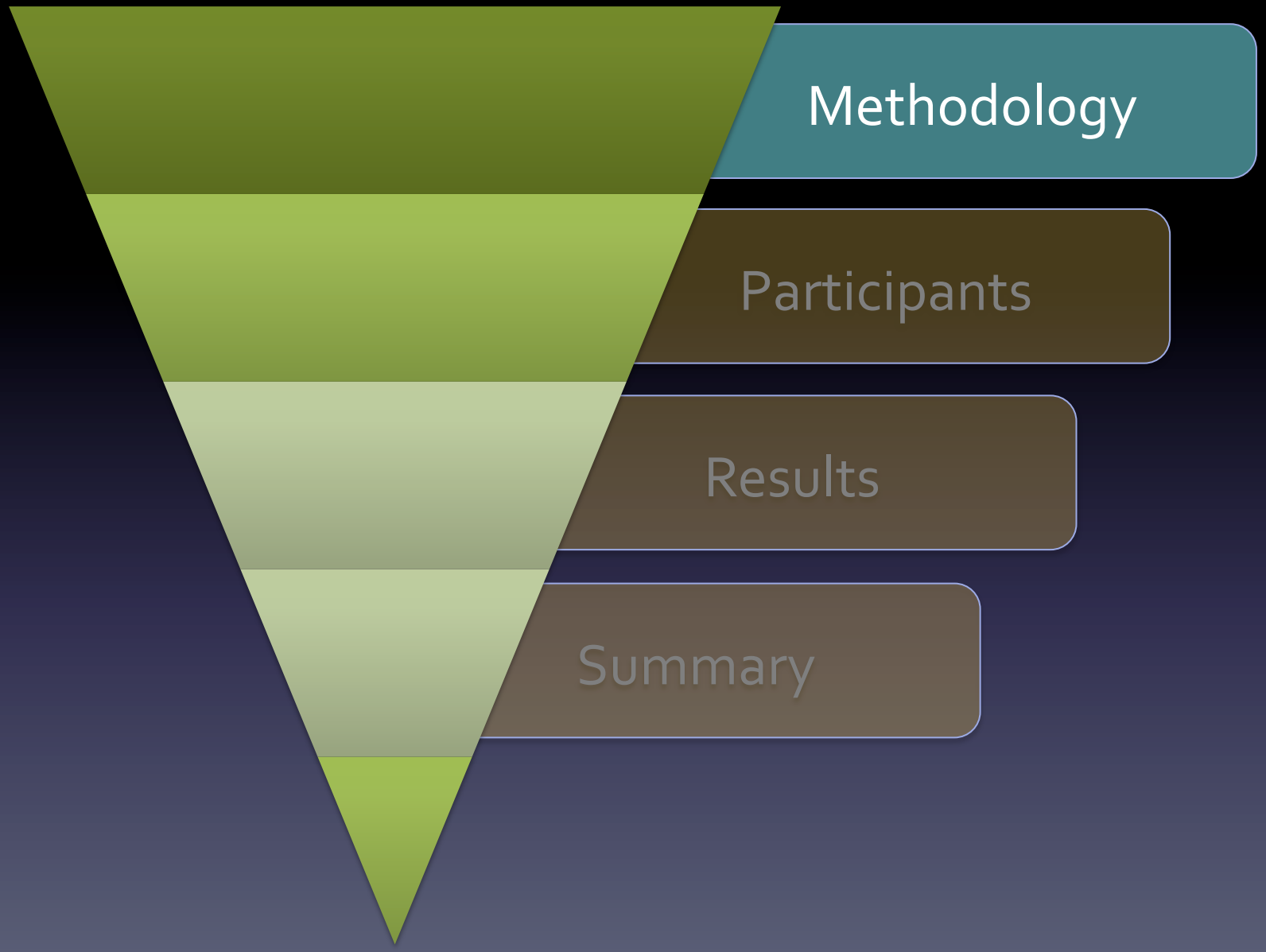


VS

Political Activists, Journalists, etc.

How do **general users** consider the **security and usability tradeoffs** between exchange and registration models?


Methodology
Participants
Results
Summary


Methodology
Participants
Results
Summary

Methodology

Participants

- Email listservs
- Online platforms, e.g. Craigslist
- Flyers

First Model

- High-level concepts
- Complete email tasks, learn about security
- Feedback

Second Model

- High-level concepts
- Complete email tasks, learn about security
- Feedback

Overall Feedback

Model Design

Mailvelope

Email Tasks for Introducing Concepts

1. Generate/Register public lock/private key pair

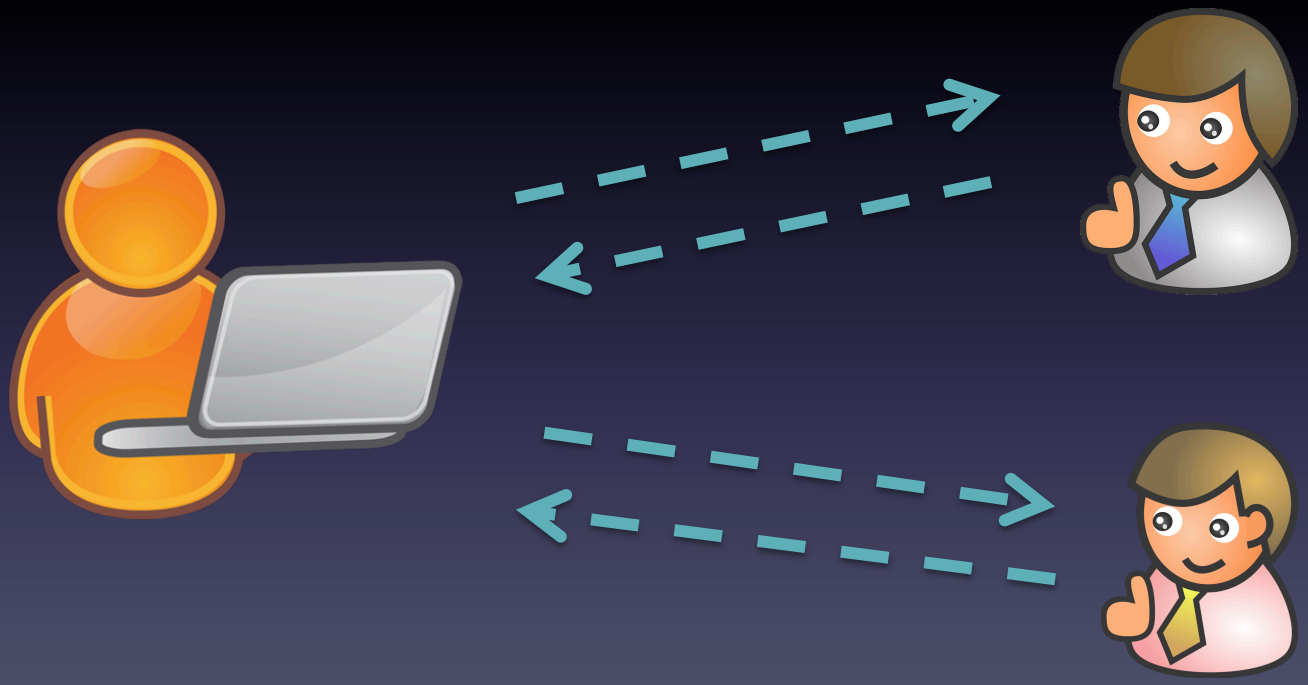
Email Tasks for Introducing Concepts

2. Exchange email with Alice

*Participants don't need to exchange public locks in the *registration model.*

Email Tasks for Introducing Concepts

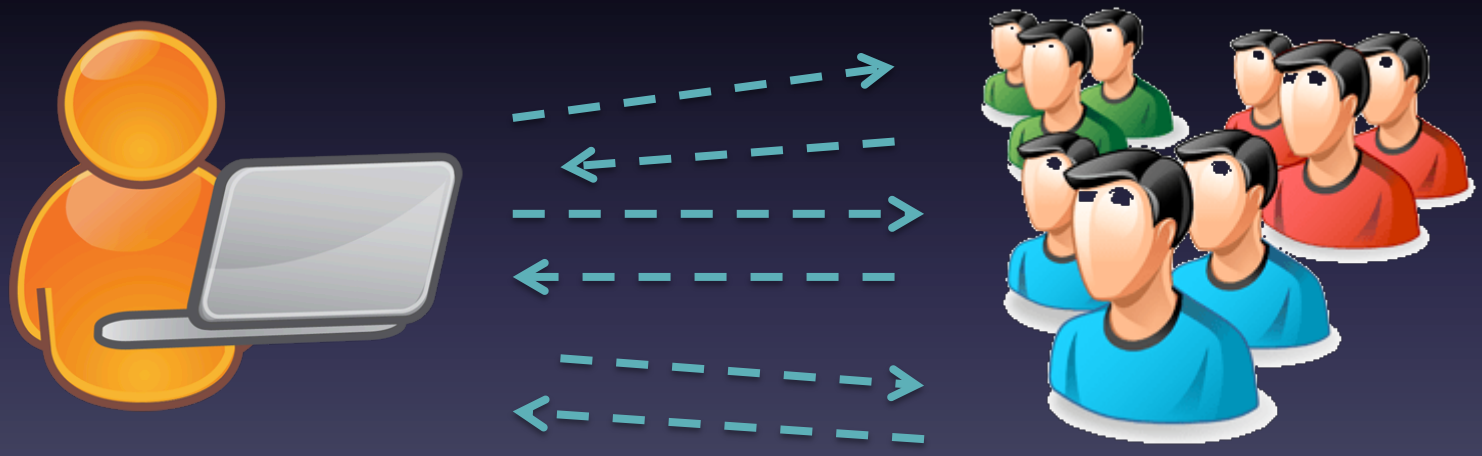
3. Exchange email with Bob and Carl



*Participants don't need to exchange public locks in the *registration model.*

Email Tasks for Introducing Concepts

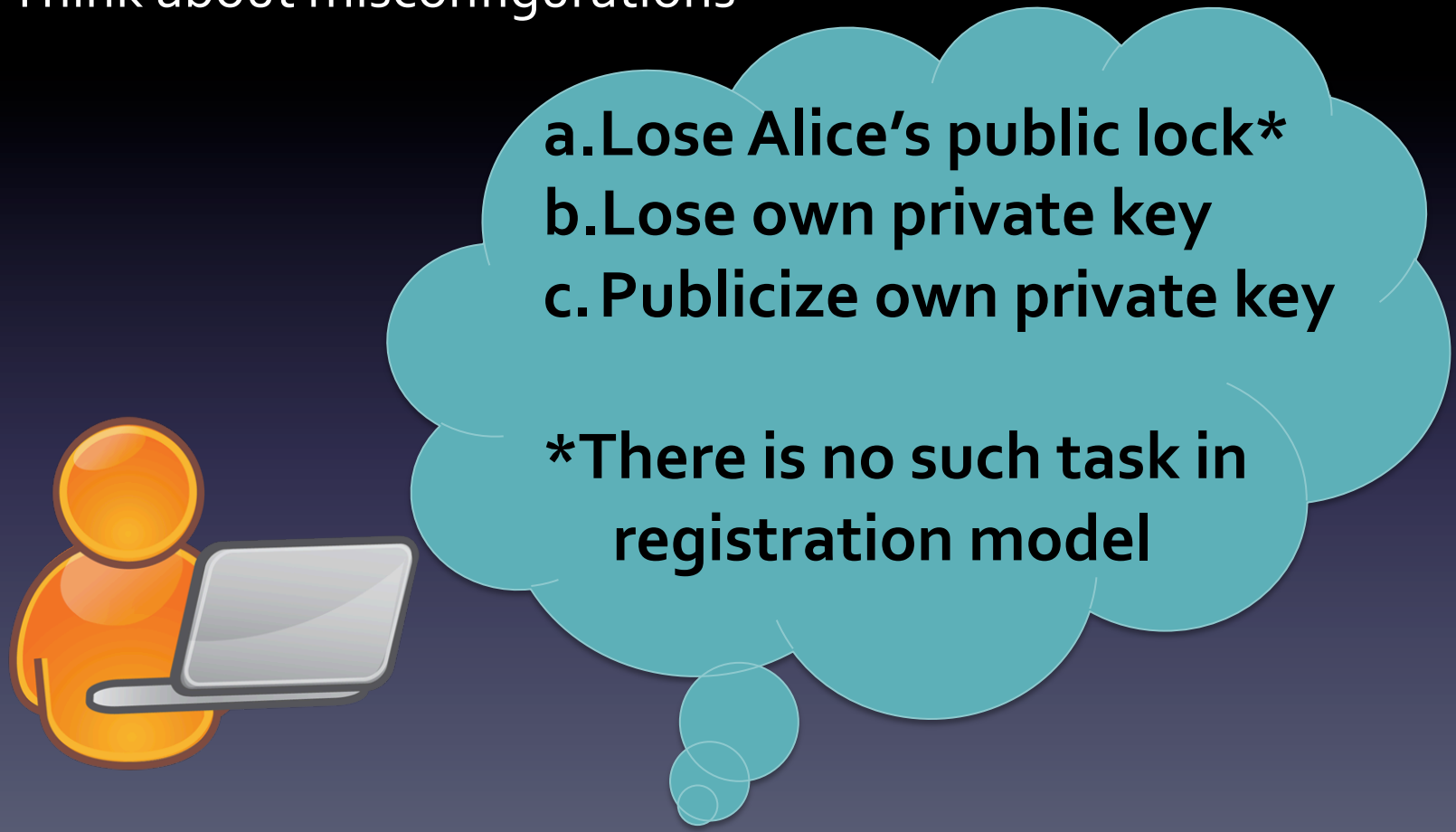
4. Imagine exchanging email with ten people



*Participants don't need to exchange public locks in the *registration model.*

Email Tasks for Introducing Concepts

5. Think about misconfigurations



Security Learning: Exchange Model

Mallet

"This threat doesn't happen usually, because it requires Mallet to have much power and resources to achieve this."

Security Learning: Registration Model (Primary)

"[In primary registration model] you need to trust the email provider"

Security Learning: Registration Model (**CaaS**[1])

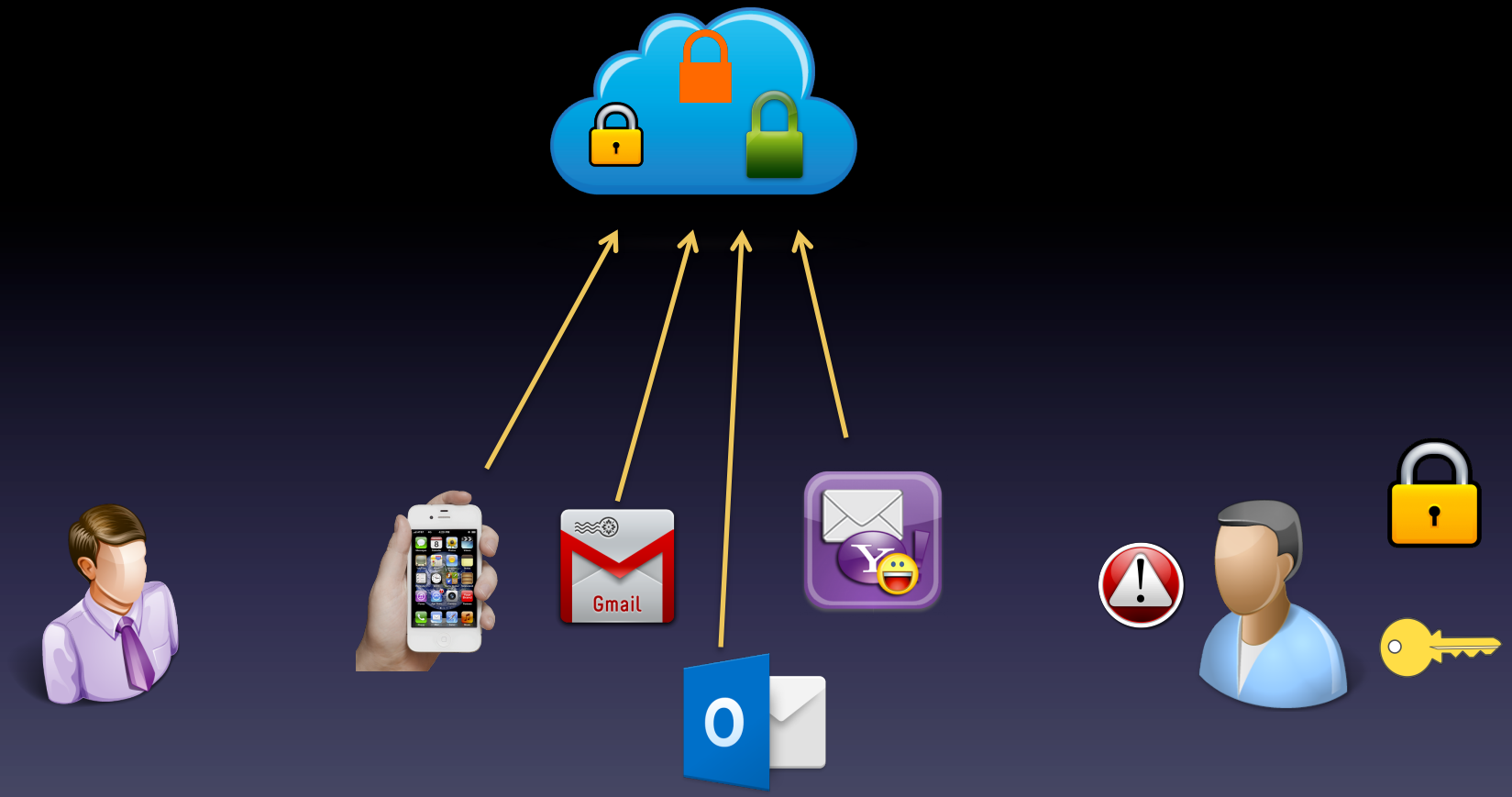
Email Provider

Third-Party Service

"[In CaaS model] you need to trust the two parties don't collaborate."

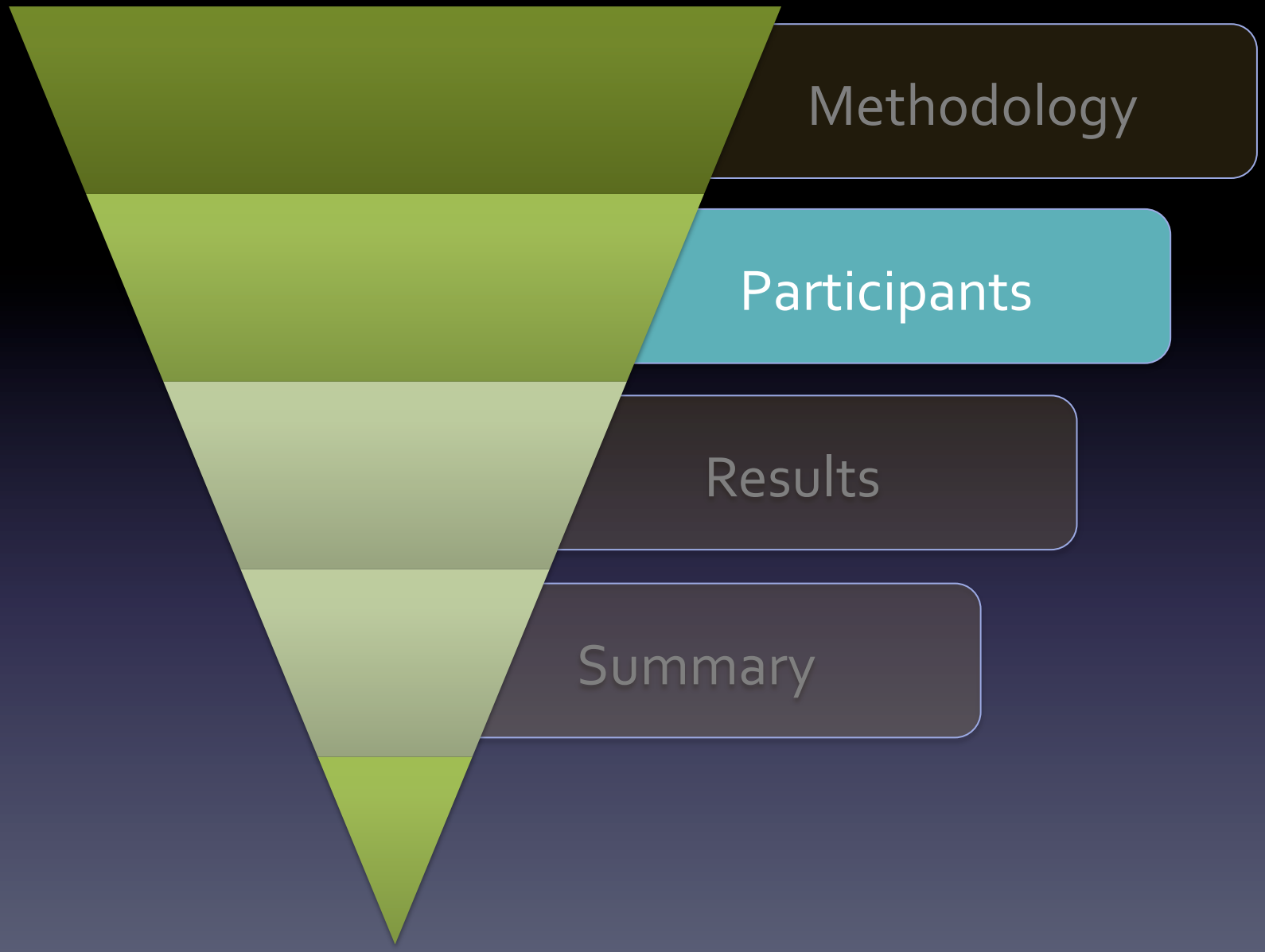
[1] S. Fahl, M. Harbach, T. Muders, and M. Smith. Confidentiality as a Service – usable security for the cloud. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pages 153–162, June 2012.

Security Learning: Registration Model (Auditing[1])



"[In auditing model] you need to trust the auditors and/or the software on your devices."

[1] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman. CONIKS: Bringing key transparency to end users. In 24th USENIX Security Symposium (USENIX Security 15), pages 383–398. USENIX Association, Aug. 2015.


Methodology
Participants
Results
Summary

Participants

80% Between Ages of 18-34

Gender:
Male 60%
Female: 40%

Occupation:
40% reported jobs or majors in computing, math and engineering

52

Participants

52

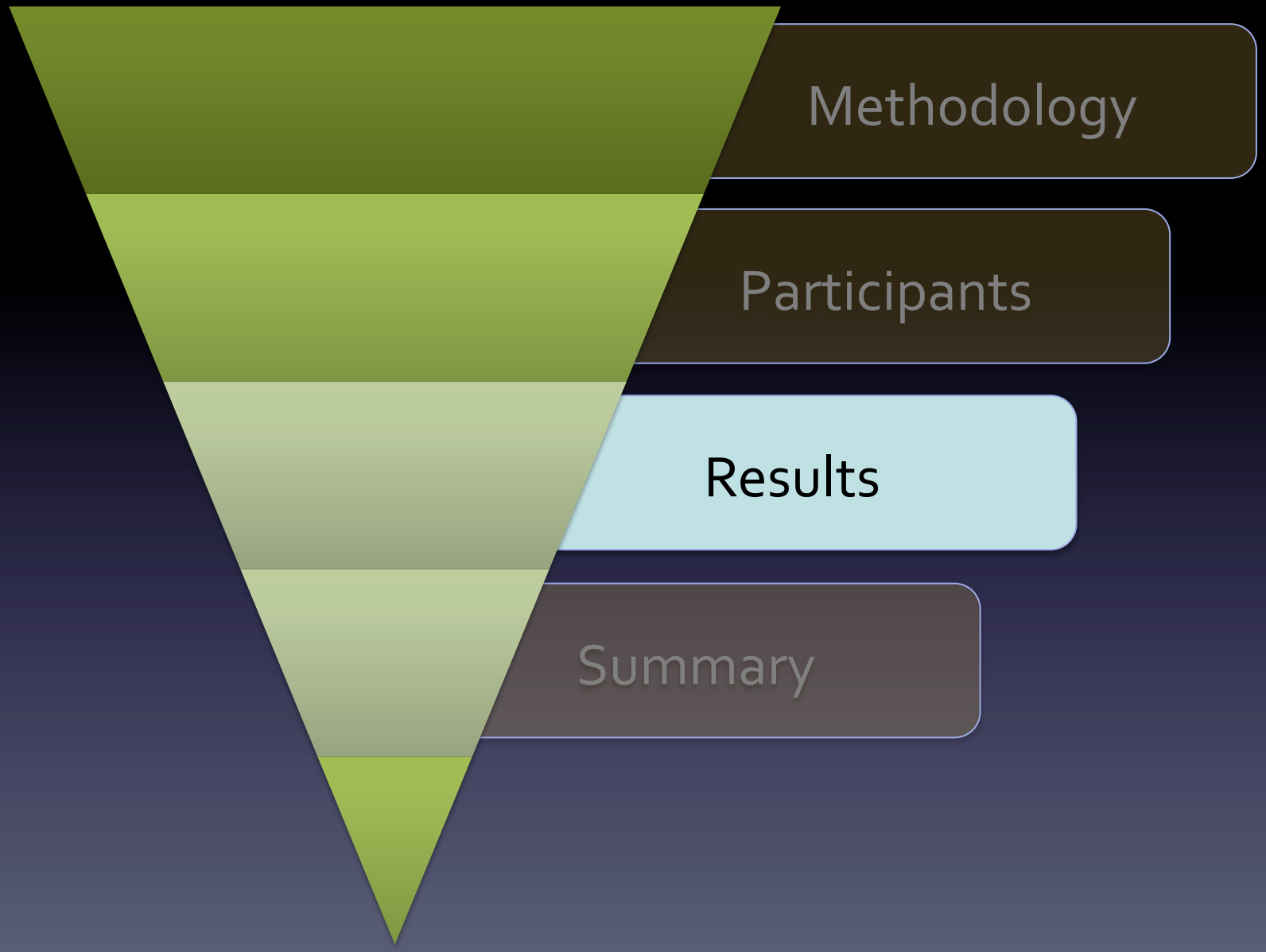
Security Expertise[1]:
2 out of 52 scored 3 or higher (out of 5.5)

[1] L. J. Camp, T. Kelley, and P. Rajivan. Instrument for measuring computing and security expertise. Technical Report TR715, Indiana University, Feb. 2015.

Analysis

- Quantitative Analysis
  - 5-point Likert scale responses
  - Cumulative-link mixed regression model (CLMM)

- Qualitative Analysis
  - Open coding independently by two researchers
  - Met to resolve all differences


Methodology
Participants
Results
Summary

Selected Results

1 Usability

2 Security

3 Comparison

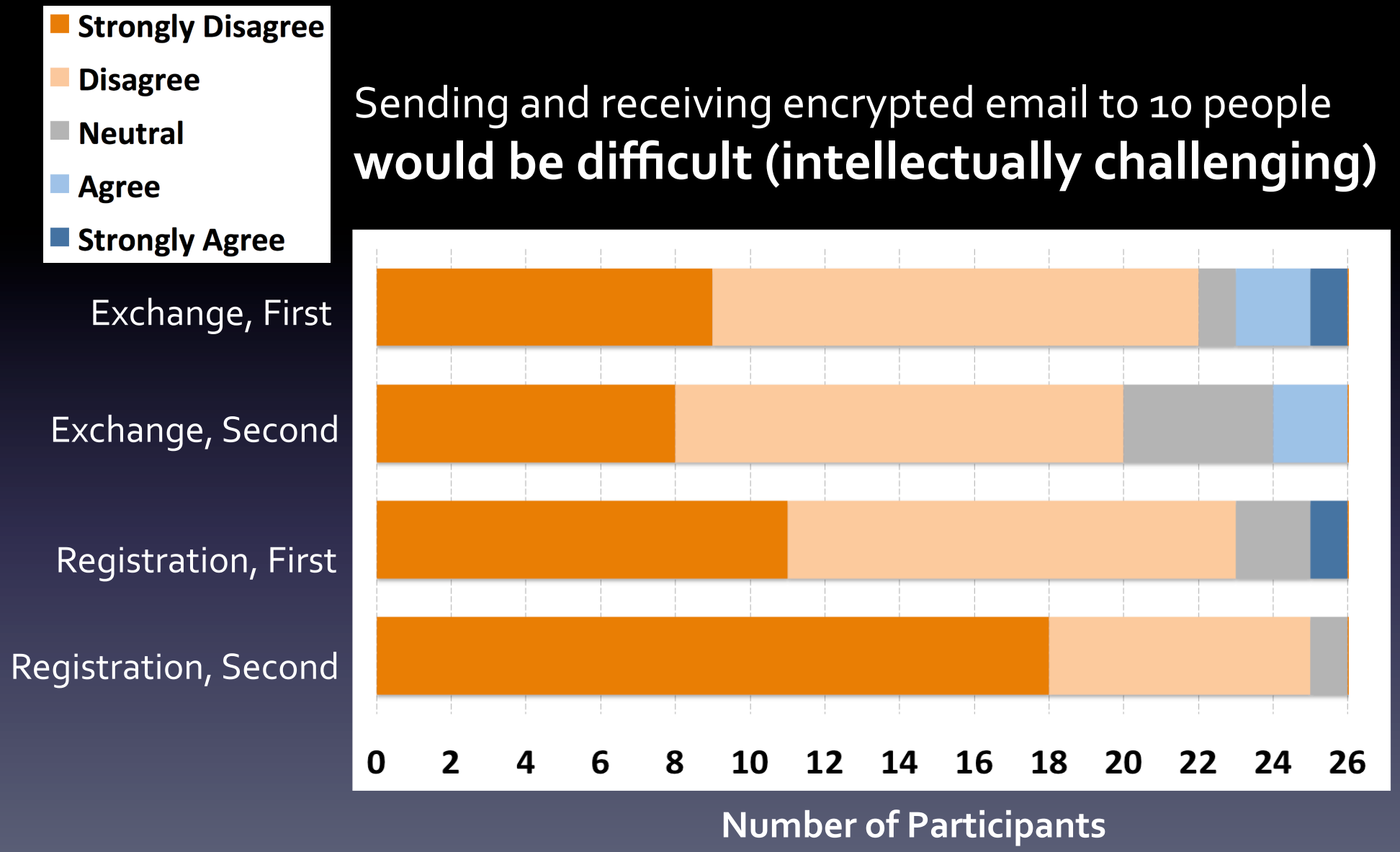
Selected Results

1 Usability

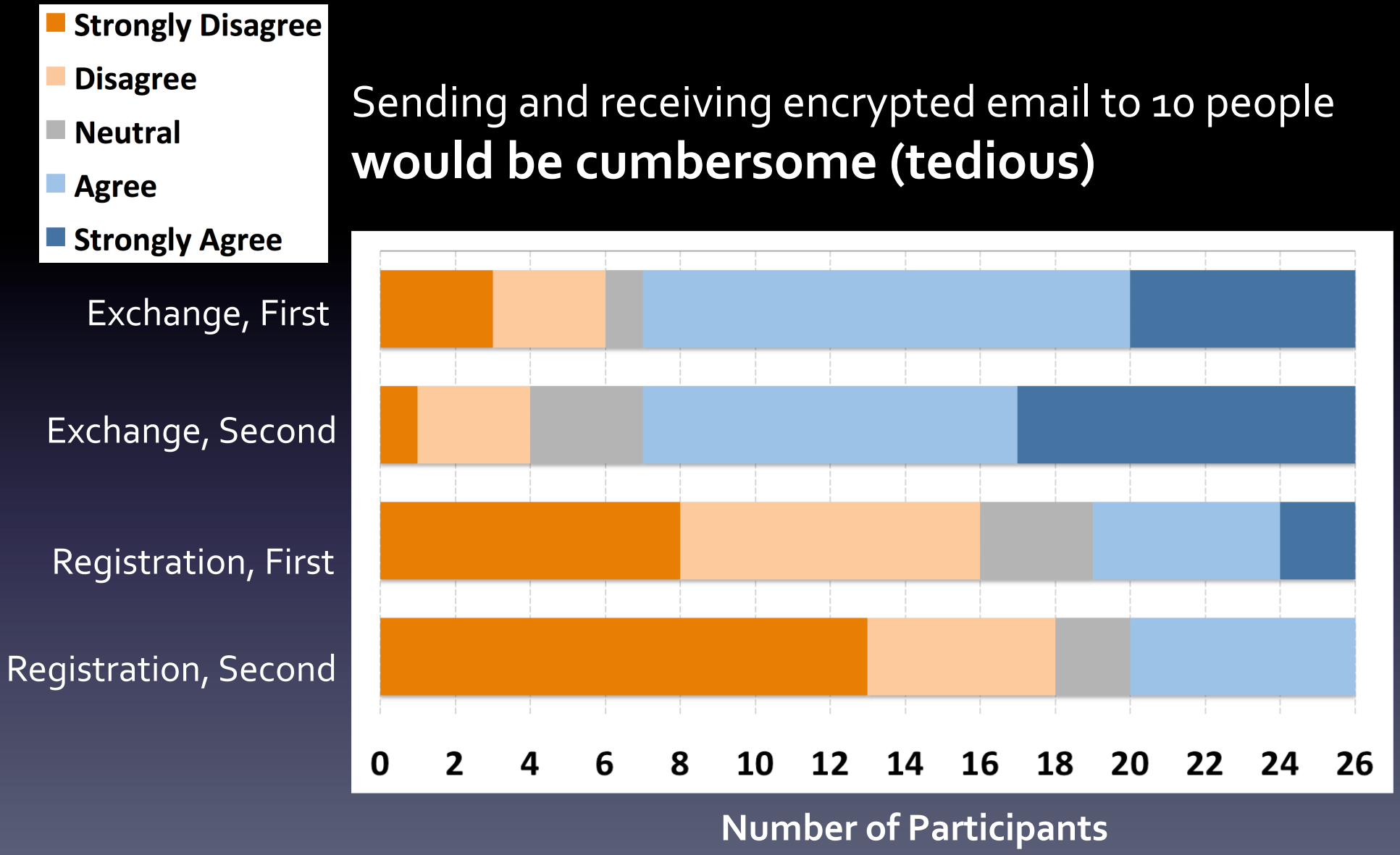
2 Security

3 Comparison

Sending and receiving encrypted email to 10 people
would be difficult (intellectually challenging)



Sending and receiving encrypted email to 10 people
would be cumbersome (tedious)



Exchange model was dramatically more cumbersome and somewhat more difficult.

"(The exchange model is) time consuming, especially sending urgent emails. I have no choice but to wait for (the correspondent's public lock)."

——ES9

Selected Results

1 **2** 3

Usability **Security** Comparison

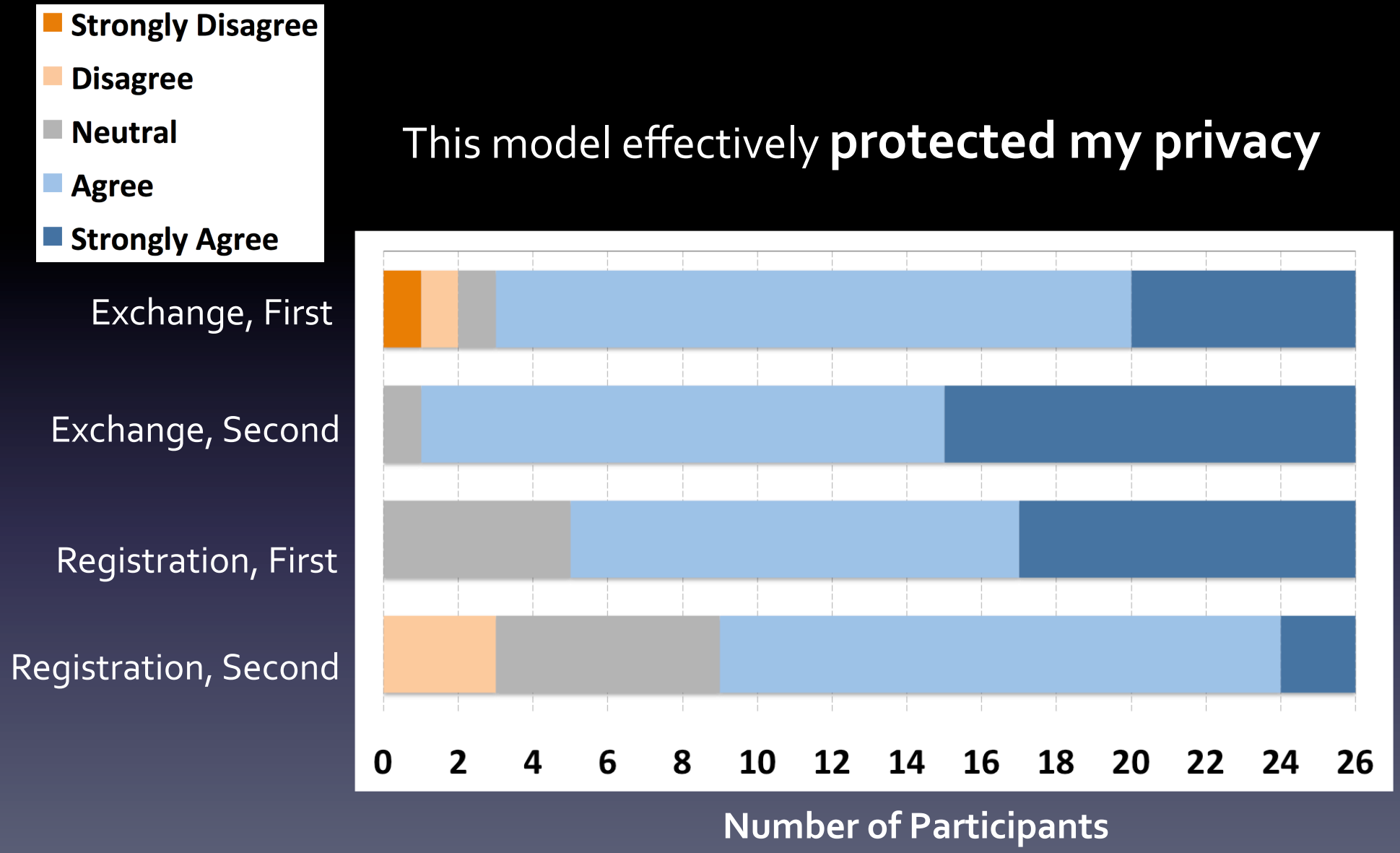
Security Comparison

The Perceived Security Gap **Is Small**

Manual effort may lead to vulnerability

Some concern but generally trusted

This model effectively **protected my privacy**



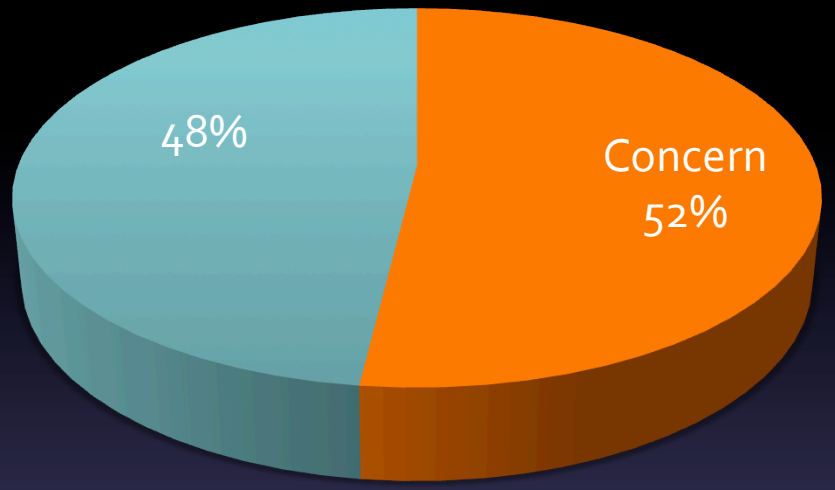
48 (out of 52) trusted *the exchange model.*

38 trusted *the registration model*.

The order participants saw each model played a significant role:

participants who saw *registration model* first were more comfortable with it.

Exchange model: manual effort may lead to vulnerability



More than half were concerned about the **security of the medium** used to exchange locks.

"There are too many exchanges between different people. Exchanging [locks] to many people may go wrong."

—— RT7

(Primary) Registration model: some concern but generally trusted

10 participants trusted their own email provider.

7 participants were specific about which kind of providers they would trust:

> "(Big companies like) Google and Yahoo! don't do such things [violate users' privacy], unless the government forces them to do so. In general, it's secure."
>
> ——RT10

CaaS and auditing models: some additional perceived security for registration

"(**In CaaS Model**) If one party is screwed up, you have another one to protect [your email]. You are still safe."

——ES8

"(**In Auditing Model**) Obviously it's extra secure. Other parties are verifying it."

——ET13

CaaS and auditing models: still some concerns

"(**In CaaS Model**) Involving more systems may complicate the system, so it is less trustful."

—— RS1

"(**In Auditing Model**) I want to know who these auditors are, . . . Their reputations, and whether they are truly independent."

——RS9

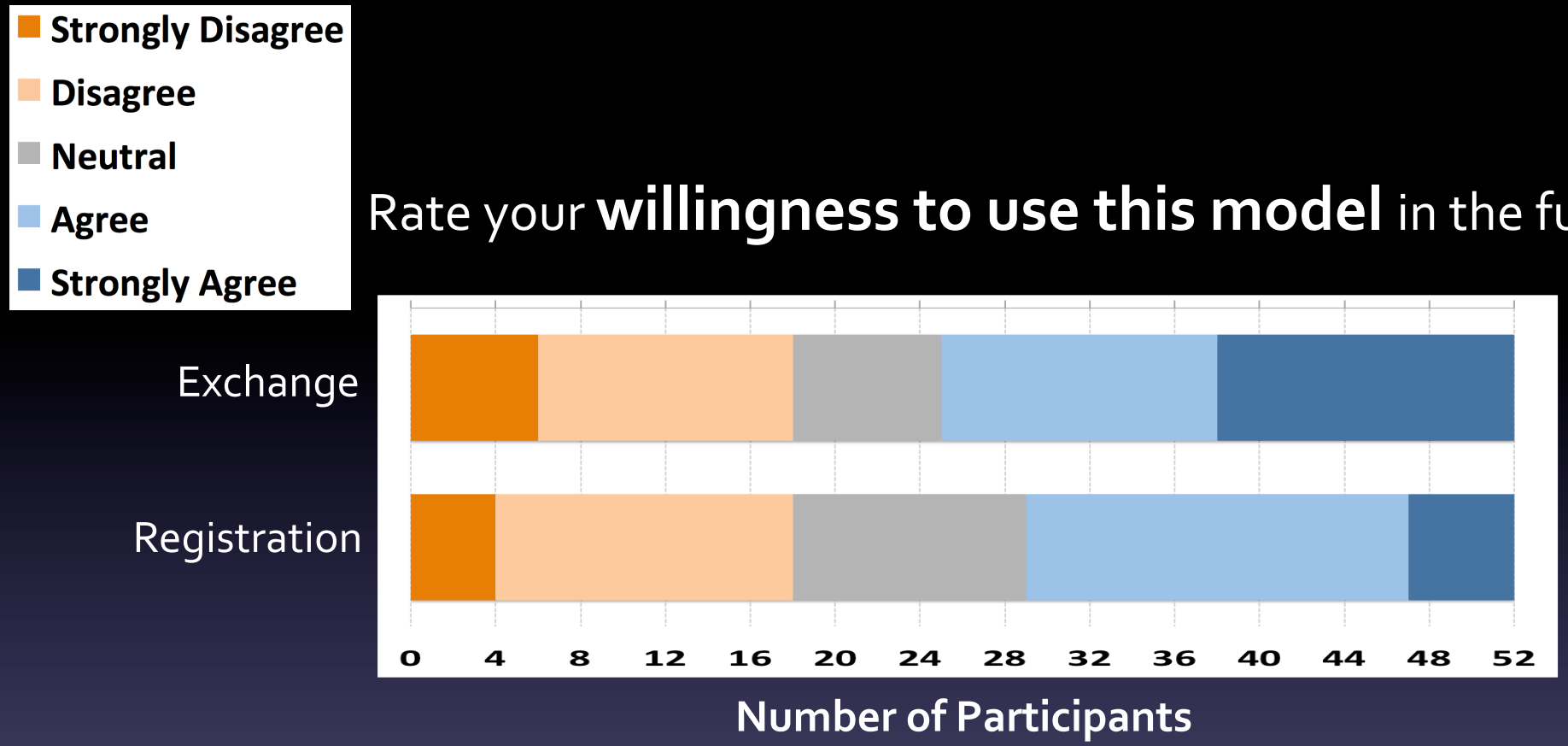
Selected Results

1 Usability

2 Security

3 Comparison

Rate your **willingness to use this model** in the future



No significant difference between two models for personal use.

When they would use the models

Registration model

- more broad use

15 would use in general email or large scale

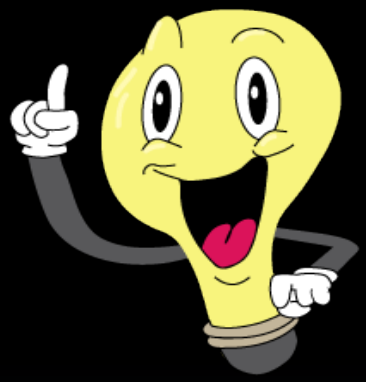
Exchange model

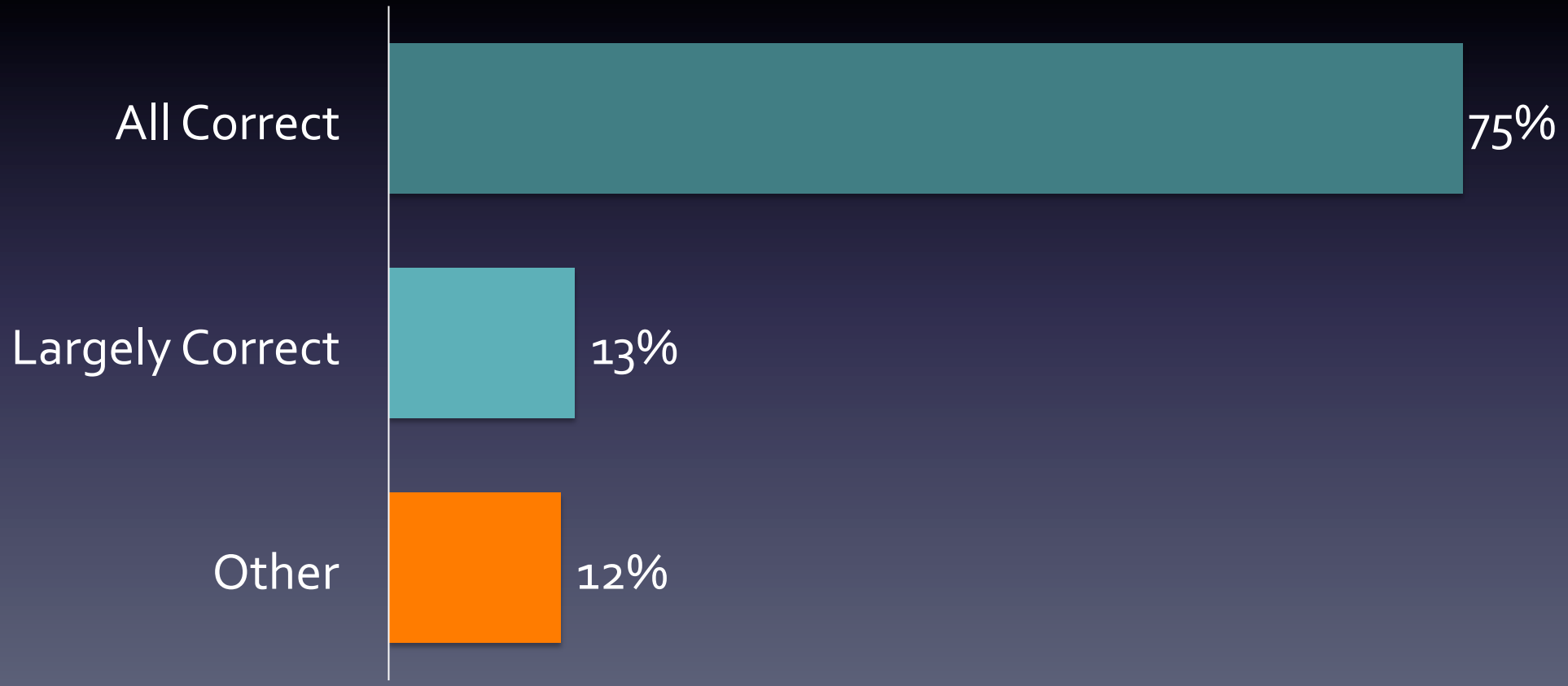
- high-security info only
- at a small scale only

1 would use in general email

0 large scale

Handling Misconfigurations





Handling Misconfigurations

Losing private key?

One participant mentioned recovering keys from a backup (such as a USB drive) rather than generating a new key pair.

"I will send my email to a third person I trust, and ask that person to encrypt the email for me and send to my recipients. Similarly, he will decrypt the [response] email for me and forward it to me."

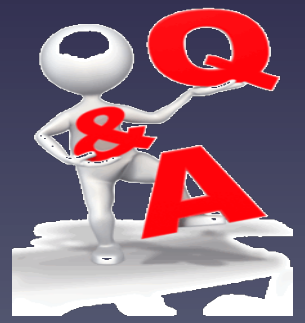
Summary

- It is **possible to explain** the high level concepts and risks of encryption to users.
- Place users in the context, and trust their decisions.
- They **can** think about tradeoffs effectively.

Summary

- *The registration model* is **more convenient** than *the exchange model*, BUT the **perceived security gap** between them is **small**.

- Show a near-best-case possibility of explaining encryption to users.



Contact: Wei Bai, University of Maryland, College Park
wbai@umd.edu