Privacy-Preserving Applications on Smartphones

Yan Huang
Peter Chapman
David Evans
University of Virginia
http://www.MightBeEvil.com

HotSec '11
August 9, 2011
What's on your phone?

Contacts

Location History

Pictures

Email

Genome (maybe next year)

Banking & Payment

Google wallet
Mutual Contact Discovery

Transfer entire (hashed) contact list between devices?
Mutual Contact Discovery

Sharing contact list with a stranger is unacceptable

Someone nearby also knows Alice and 8 other contacts of yours!
The Dilemma

Can we interact with others and control our data?
Trust a Third Party?

- SEGA: June 2011, 1.3 Million
- SONY: April 2011, 70 Million
- Citi: June 2011, 200,000
- epsilon: April 2011, 2,500 Corporate Clients
- Dropbox: June 2011, 25 Million
Secure Two-Party Computation

Bob (circuit evaluator)
Private Data: $a$

Agree on
$f(a, b) \rightarrow x$

Alice (circuit generator)
Private Data: $b$

Garbled Circuit Protocol

Outputs $x = f(a, b)$ without revealing $a$ to Bob or $b$ to Alice.

Semi-honest threat model

Andrew Yao, 1982/1986
Potential Applications

Two Party
Common Contacts
Favorite Workshop Papers

Multi-Party
Voting, Auctions & more!
Collaborative Scheduling

Hyper-Targeted Advertising
Potential Applications

User-Initiated (Explicit)  Automatic (Background)

Voting, Auctions & more!
Favorite Workshop Papers
Common Contacts
Hyper-Targeted Advertising
Collaborative Scheduling
Implementing Privacy-Preserving Applications
Secure-Computation Framework

Faster Secure Two-Party Computation Using Garbled Circuits
Yan Huang, David Evans, Jonathan Katz, & Lior Malka

Available now:
http://mightbeevil.org/framework/

See our talk in the Friday, 5 PM Applied Cryptography
USENIX Security technical session:

Faster Secure Two-Party Computation Using Garbled Circuits
Yan Huang, David Evans, Jonathan Katz, & Lior Malka

Java-Based Garbled Circuit Framework
Pipelined Circuit Execution
Free XOR
Circuit-Level Optimizations
Porting the Framework

100 non-free gates per second: 1000 times slower than desktop!

No cryptographic hardware modules.

We thank Google for the Nexus One phones!
Common Contacts

Search for mutually shared contacts, without leaking others.

24-bit Hashes of Email and Phone Numbers

Sort-Compare-Shuffle to do private set intersection in $O(n \log n)$

128 contacts compared in 150 seconds
Java's immutable BigInteger causes 1/2 of time to be spent on GC
Improving Mobile Performance

Poster and Demo: *More Efficient Secure Computation on Smartphones*
Sang Koo, Yan Huang, Peter Chapman, and David Evans
(Thursday, 6PM California East/West)

Java's *immutable* BigInteger causes 1/2 of time to be spent on GC
Future Optimization: RenderScript

C99 with extensions

Runs on either CPU or GPU depending on complexity

Renderscript transform test
Displaying file: R.raw.robot
Future Directions
Stronger Adversaries

Semi-Honest (Honest But Curious) Adversary
Adversary follows the protocol as specified (!)
Curious adversary tries to learn more from protocol execution transcript.
Stronger Adversaries

**Semi-Honest (Honest But Curious) Adversary**

Adversary follows the protocol as specified (!)

Curious adversary tries to learn more from protocol execution transcript.

_Semi-Honest Good Enough?_
Stronger Adversaries

**Semi-Honest (Honest But Curious) Adversary**

Adversary follows the protocol as specified (!)
Curious adversary tries to learn more from protocol execution transcript.

Semi-Honest Good Enough?

Software Based Attestation?
Leveraging the Carrier

Any new peers nearby?

Carriers can identify and locate devices on their networks.
OS Support for Secure Computation

Private data restricted to secure computation by OS

OS/Standardized Displays
Summary

• Useful applications that are “social” and cryptographically protect privacy.

• Performance challenges, open research questions, and deployment hurdles remain.
http://MightBeEvil.com/mobile/
User-Friendly Secure Computation

User Education

OS/Standardized Displays

Private data restricted to secure computation by OS
Application Development

**Now:** Privacy-Preserving computations as a concept must break out of academia

Proper education about data leakage and threat mode

**+2 Years:** Secure Computation Library Development

Share Sub-circuits & Components

**+5 Years:**
Automatic Source Conversion with Privacy-Preserving Functionality
Heterozygous Recessive Risk

Goal: Compute overall risk across a range of diseases

Noncarrier: 25%
Just Carrier: 50%
Disease: 25%

cystic fibrosis
Background Secure Computations

Do we go to the same bars?

Do we share the same interests?

I just watched all of Arrested Development on Hulu, got any deals?

Must cap repeated executions