Privacy-Enabling Social Networking Over Untrusted Networks

Jonathan Anderson, Claudia Diaz*, Joseph Bonneau and Frank Stajano

{jonathan.anderson,joseph.bonneau,frank.stajano}@cl.cam.ac.uk
claudia.diaz@esat.kuleuven.be

Computer Laboratory

* K.U. Leuven ESAT/COSIC
Outline

• Social networks require absolute trust
• Operators don’t protect their users
• Smart clients can protect themselves
  • Protocols
  • Privacy
  • Performance
Social Networks Require Absolute Trust
Social Networks Require Absolute Trust
Social Networks Require Absolute Trust
Social Networks Require Absolute Trust
Social Networks Require Absolute Trust
Social Networks Require Absolute Trust
Network Operators Don’t Protect Their Users

Facebook's Beacon More Intrusive Than Previously Known

A Computer Associates security researcher says that Facebook's controversial system goes much further than expected in tracking people's Web activities.

Facebook's "Secret Crush" malicious widget trick

Facebook users faked into downloading adware, security firm says

By Ellen Messmer, Network World, 01/03/2008

Facebook Retracts on Online Tracking

By LOUISE STORY and BRAD STONE
Published: November 30, 2007

Facebook suspends app that permitted peepholes

by Elinor Mills

Facebook shrugs off warning to vet potentially malicious programs

Social networking site's users under attack from programs seeking to steal personal data, says expert

Jemima Kiss
 guardian.co.uk, Monday 2 March 2009 17.25 GMT
Article history
Smart Clients Can Protect Themselves

• Stop trusting the network!
• Smart clients, dumb servers
How Do You Facebook?
How Do You Facebook?

Pigs Fly As Facebook And Google Work Together On An Android App

by Erick Smith

Well, we read recently on the new service Facebook and Google are working on: an app for Android phones. We can only imagine the popping up of apps as they work to confirm our fears. We have a feeling the Google Market (it's still not quite official) will be just as the end result. However, seeing Facebook's limited set of services that are still very popular, it isn't too hard to have an inkling what's ahead.
Decentralised Architecture
Decentralised Architecture
Decentralised Architecture
Privacy Requirements

• Protect **content** and **links**

• Adversaries:
  • Other users
  • Application developers
  • Network operator

• Reduce to social contract
Application Layer

• Sandboxed applications
• Security API
  • Restrictive default policies
  • User policy specification
Profile Data


550e8400-e29b-41d4-a716-446655440000
550e8400-e29b-41d4-a716-446655440000
550e8400-e29b-41d4-a716-446655440000
550e8400-e29b-41d4-a716-446655440000
Data Structures Layer
Data Structures Layer
Data Structures Layer
Data Structures Layer
Software Architecture
Cryptography Layer

- Encryption, digital signatures, etc.
- Key Management
- Identity Verification
- Link Hiding
Encrypted Blocks

• Unique symmetric key per block per ACL revision
• This sounds familiar...
• No revocation guarantees
Key Management

• Direct distribution via PK
• Key hierarchy
  • “Group key” blocks
• Hidden links
Link Hiding

03 00 4d 0b 59 7a e5 b0 7a bf 89 c8 f6 b0 2d
74 76 2d 30 64 67 9a 42 f6 34 15 bc 66 71 91
2a 34 0e e6 45 c4 ff 8f d7 90 95 4a e3 a8 2e
Link Hiding

\[ \begin{array}{c}
K_1 \rightarrow E \\
\downarrow \\
\uparrow \\
K_2 \rightarrow E
\end{array} \]

\[
\begin{array}{c}
03 \ 00 \ 4d \ 0b \ 59 \ 7a \ e5 \ b0 \ 7a \ bf \ 89 \ c8 \ f6 \ b0 \ 2d \\
74 \ 76 \ 2d \ 30 \ 64 \ 67 \ 9a \ 42 \ f6 \ 34 \ 15 \ bc \ 66 \ 71 \ 91 \\
2a \ 34 \ 0e \ e6 \ 45 \ c4 \ ff \ 8f \ d7 \ 90 \ 95 \ 4a \ e3 \ a8 \ 2e
\end{array}
\]
Link Hiding

03 00 4d 0b 59 7a e5 b0 7a bf 89 c8 f6 b0 2d
74 76 2d 30 64 67 9a 42 f6 34 15 bc 66 71 91
2a 34 0e e6 45 c4 ff 8f d7 90 95 4a e3 a8 2e

K₁ → E

K₂ → E
Link Hiding

03 00 4d 0b 59 7a e5 b0 7a bf 89 c8 f6 b0 2d
74 76 2d 30 64 67 9a 42 f6 34 15 bc 66 71 91
2a 34 0e e6 45 c4 ff 8f d7 90 95 4a e3 a8 2e

K₁ → E

1e fb L I N K : a b c . . . 92 71 44
99 1c ff bf d9 5a e1 03 08 8e 7d 9b c2 45 56
aa dd 0e 64 fc 7f a3 c4 77 77 e6 a0 81 c4 5a

K₂ → E

ad e6 e1 69 fd 4e 70 3c da ce f8 c6 94 0f e7
3c 6b 66 c5 39 6c 1c 74 c1 14 ef 53 L I N
K : d e f . . . 70 32 22 12 37 9d 92 e4
Messaging

- Asynchronous
  - Encryption
  - Signing
- Synchronous
  - OTR
Identity Verification

- PKI
- Web of Trust
- Fingerprint Exchange
- Multi-Channel Protocol
Fingerprint Exchange

- CryptoIDs
  - “a little longer than most email addresses, a little shorter than most postal addresses, and about the same size as a credit card plus its 4-digit expiration date”
  - f3v4g.ifcen.r3rj5.embx8
  - small enough for a business card
Mutual Identity Verification

- Wong-Stajano protocol
- Exchange of small nonces
  - Nonces can be cryptographically weak
  - Relies on data origin authenticity
Joint Content

- Digital signature convention
- Sign content and context
Software Architecture

- Application
- Application API
- Data Structures
- Cryptography
- Server API
- TCP/IP
Network Layer

- GET, POST
- Access control
  - **Not** for confidentiality
  - Ok for integrity
- Extra: mailboxes?
Implementation

Loading Safebook

When Safebook has finished loading, you should be redirected. If not, try clicking this link.
Implementation

Loading Safebook

When Safebook has finished loading, it may prompt for permission to access your computer. The digital signature could not be verified. Click "Details..." for more information or "Deny" to block access.
Implementation
Performance

- Server
  - Storage scales (roughly) linearly with users
  - Computation scales linearly with storage
- I/O-bound clients (branching factor)
Open Problems

- Usability of policy specification
- End user development
- Security API
Appendix

• Wong-Stajano protocol
• Crypto performance
Wong-Stajano Protocol

\[ \begin{align*}
A &\rightarrow B : K_A \\
B &\rightarrow A : K_B \\
A &\rightarrow B : H(A | K_A | K_B | R_a | K_a) \\
B &\rightarrow A : H(B | K_A | K_B | R_b | K_b) \\
A &\Rightarrow B : R_a \\
B &\Rightarrow A : R_b \\
A &\rightarrow B : K_a \\
B &\rightarrow A : K_b \\
A &\Rightarrow B : \text{outcome} \\
B &\Rightarrow A : \text{outcome}
\end{align*} \]
Crypto Performance

- SunJCE v1.7 on Intel Core2 Quad CPU Q6600 @ 2.4 GHz
- RSA
  - 1024b en/decryption @ 600 kB/s, 30 kB/s
  - 2048b RSA en/decryption @ 200 kB/s, 7 kB/s
- AES: 128b @ 35 MB/s