Towards Perfectly Secure and Deniable Communication Using an NFC-Based Key-Exchange Scheme

Daniel Bosk[1] Martin Kjellqvist[2] Sonja Buchegger[1]

[1] KTH Royal Institute of Technology
{dbosk,buc}@kth.se

[2] Mid Sweden University
martin.kjellqvist@miun.se

NordSec'15, Stockholm, 20th October 2015

Overview

1. What's the Problem?
   - Background
   - What we want to do?
   - What part of the problem do we solve?
2. Why is this a problem?
   - Because Eve has lots of power
3. How to solve this?
   - A Protocol
   - The Security of the Protocol
   - Implementation and Evaluation
4. Conclusions
   - Our Contributions

Overview

Modern Surveillance

- We've learned a lot about modern surveillance states since 2013.
  - Tapping fibre-optic cables [4]
  - Storing all intercepted data [1]
  - Search [2] and visualization [3] capabilities of intercepted data.
- Basically they build an Internet-wide transcript of all communications.

Modern Surveillance

- We've learned a lot about modern surveillance states since 2013.
  - Tapping fibre-optic cables [4]
  - Storing all intercepted data [1]
  - Search [2] and visualization [3] capabilities of intercepted data.
- Basically they build an Internet-wide transcript of all communications.

What we want to do?

- Alice and Bob communicate.
- Eve records everything.
- Eve forces Alice to give her a key to decrypt the transcripts.
- Alice doesn't like this.
- Alice wants to give Eve a key $k' \neq k$ such that $\mathrm{Dec}_{k'}(c) = m'$.

What we want to do?

- Alice and Bob communicate.
- Eve records everything.
- Eve forces Alice to give her a key to decrypt the transcripts.
- Alice doesn't like this.
- Alice wants to give Eve a key $k' \neq k$ such that $\text{Dec}_{k'}(c) = m'$.

What we want to do?

- Alice and Bob communicate.
- Eve records everything.
- Eve forces Alice to give her a key to decrypt the transcripts.
- Alice doesn't like this.
- Alice wants to give Eve a key $k' \neq k$ such that $\mathrm{Dec}_{k'}(c) = m'$.

Popular PETs

- GNU Privacy Guard (GPG), Off-the-Record (OTR), TextSecure, . . .
- GPG has no claimed deniability.
- OTR and TextSecure has Perfect Forward-Secrecy (PFS).
- This requires "innocent until proven otherwise".
- What if we're "guilty until proven otherwise"?

Popular PETs

- GNU Privacy Guard (GPG), Off-the-Record (OTR), TextSecure, . . .
- GPG has no claimed deniability.
- OTR and TextSecure has PFS.
- This requires “innocent until proven otherwise”.
- What if we’re “guilty until proven otherwise”?

Popular PETs

- GNU Privacy Guard (GPG), Off-the-Record (OTR), TextSecure, . . .
- GPG has no claimed deniability.
- OTR and TextSecure has PFS.
- This requires "innocent until proven otherwise".
- What if we're "guilty until proven otherwise"?

Popular PETs

- GNU Privacy Guard (GPG), Off-the-Record (OTR), TextSecure, . . .
- GPG has no claimed deniability.
- OTR and TextSecure has PFS.
- This requires "innocent until proven otherwise".
- What if we're "guilty until proven otherwise"?

How do we go about?

- A public channel, e.g. the Internet.
- A private channel, e.g. Near-Field Communication (NFC).

What can Eve do?

- Eve records everything in the public channel.
- She also stores this indefinitely.
- But Eve cannot record anything in the private channel.

What can Eve do?

- Eve records everything in the public channel.
- She also stores this indefinitely.
- But Eve cannot record anything in the private channel.

What can Eve do?

- In related works, Eve has had the role of prosecutor.
- She has to convince a third-party judge.
- In our model, Eve is both prosecutor and judge.
- Which is more the case in some surveillance states.
- There is a formal definition of this in the paper . . .

What can Eve do?

- In related works, Eve has had the role of prosecutor.
- She has to convince a third-party judge.
- In our model, Eve is both prosecutor and judge.
- Which is more the case in some surveillance states.
- There is a formal definition of this in the paper . . .

What can Eve do?

- In related works, Eve has had the role of prosecutor.
- She has to convince a third-party judge.
- In our model, Eve is both prosecutor and judge.
- Which is more the case in some surveillance states.
- There is a formal definition of this in the paper . . .

Overview

Verifying who sent what

Eve has a transcript of all that has happened on the network . . .

Verifying encryption keys

- Alice says she used key k'.
- Eve computes $\mathrm{MAC}_{H_M(k')}(c) \neq t = \mathrm{MAC}_{H_M(k)}(c)$ and says: No, you didn't.

Verifying encryption keys

- Alice says she used key k'.
- Eve computes $\mathrm{MAC}_{H_M(k')}(c) \neq t = \mathrm{MAC}_{H_M(k)}(c)$ and says: No, you didn't.

How hard is deniability?

1. Given m', c
   - find x such that $\mathrm{Enc}_x(m') = c$.
2. Given c, x as above, y such that $\mathrm{MAC}_y(c) = t$,
   - find k' such that $H_E(k') = x$ and $H_M(k') = y$.

How hard is deniability?

1. Given m', c
   - find x such that $\mathrm{Enc}_x(m') = c$.
2. Given c, x as above, y such that $\mathrm{MAC}_y(c) = t$,
   - find k' such that $H_E(k') = x$ and $H_M(k') = y$.

Overview

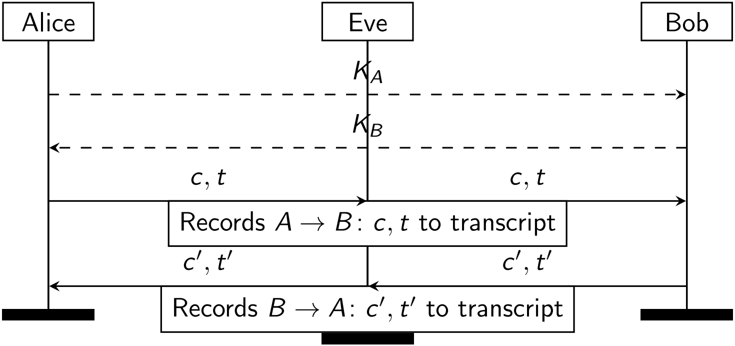

Figure: Keys K_A, K_B. Ciphertext $c = \mathrm{Enc}(m)$. MAC-tag $t = \mathrm{MAC}(c)$. c', t' correspondingly.

A rough outline

Define: Eve (formally).

A rough outline

Show: Deniable Encryption $\circ$ Encrypt-then-MAC $\implies$ Deniable Encryption

A rough outline

- Assume a *stateful deniable authenticated encryption scheme*.
- Show: such scheme gives Eve negligible advantage.
- Show: such scheme yields IND-SFCCA (indistinguishability under stateful chosen ciphertext attack).

A rough outline

- Assume a *stateful deniable authenticated encryption scheme*.
- Show: such scheme gives Eve negligible advantage.
- Show: such scheme yields IND-SFCCA (indistinguishability under stateful chosen ciphertext attack).

A rough outline

- Assume a *stateful deniable authenticated encryption scheme*.
- Show: such scheme gives Eve negligible advantage.
- Show: such scheme yields IND-SFCCA (indistinguishability under stateful chosen ciphertext attack).

A rough outline

- Define: stateful OTP.
- Show: stateful OTP $\implies$ IND-SFCCA.
- Define: stateful MACs.
- Show: stateful MACs $\implies$ INT-SFCTXT (integrity for stateful ciphertexts).

A rough outline

- Define: stateful OTP.
- Show: stateful OTP $\implies$ IND-SFCCA.
- Define: stateful MACs.
- Show: stateful MACs $\implies$ INT-SFCTXT (integrity for stateful ciphertexts).

One-Time Pad, practically feasible?

- How much random data do we need for everyday messaging?
- How long does it take to transfer using NFC?
- How difficult is it to generate this data? Will it drains the phone's battery?

One-Time Pad, practically feasible?

- How much random data do we need for everyday messaging?
- How long does it take to transfer using NFC?
- How difficult is it to generate this data? Will it drains the phone's battery?

One-Time Pad, practically feasible?

- How much random data do we need for everyday messaging?
- How long does it take to transfer using NFC?
- How difficult is it to generate this data? Will it drains the phone's battery?

How practical?

Freq	Time	Key-material (KiB)
Daily	5 s	283 KiB
Weekly	38 s	2 MiB
Monthly	3 min	8 MiB
Bimonthly	5 min	17 MiB
Annually	33 min	101 MiB

Overview

What did we achieve?

- We assume a stronger adversary model.
- We show that OTR-like protocols are not fully deniable.
- We outline the properties needed for a fully deniable protocol.
- We design a protocol with a superset of the properties of Off-the-Record (OTR):
  - authenticated,
  - yet with deniable encryption, and
  - perfectly secret.
- The protocol is based on the OTP.
- We show that the key-exchange is feasible.

What did we achieve?

- We assume a stronger adversary model.
- We show that OTR-like protocols are not fully deniable.
- We outline the properties needed for a fully deniable protocol.
- We design a protocol with a superset of the properties of OTR:
  - authenticated,
  - yet with deniable encryption, and
  - perfectly secret.
- The protocol is based on the OTP.
- We show that the key-exchange is feasible.

What did we achieve?

- We assume a stronger adversary model.
- We show that OTR-like protocols are not fully deniable.
- We outline the properties needed for a fully deniable protocol.
- We design a protocol with a superset of the properties of OTR:
  - authenticated,
  - yet with deniable encryption, and
  - perfectly secret.
- The protocol is based on the OTP.
- We show that the key-exchange is feasible.

What did we achieve?

- We assume a stronger adversary model.
- We show that OTR-like protocols are not fully deniable.
- We outline the properties needed for a fully deniable protocol.
- We design a protocol with a superset of the properties of OTR:
  - authenticated,
  - yet with deniable encryption, and
  - perfectly secret.
- The protocol is based on the OTP.
- We show that the key-exchange is feasible.

Some obstacles . . .

- Streaming not possible using NFC.
- The API requires files to be transferred.
- These files have to reside in the publicly accessible file system.

Some obstacles . . .

- Streaming not possible using NFC.
- The API requires files to be transferred.
- These files have to reside in the publicly accessible file system.

Questions?

1. Greenberg, A.: Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It. Forbes (2013)
2. Greenwald, G.: XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. The Guardian (2013)
3. Greenwald, G., MacAskill, E.: Boundless Informant: the NSA's secret tool to track global surveillance data. The Guardian (2013)
4. MacAskill, E., Borger, J., Hopkins, N., Davies, N., Ball, J.: GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian (2013)