Advanced Authentication

- Off-the-record communication -

CIS 590/798: Secure Networks and Distributed Systems

Fall 2011

Alex Bardas
Today’s Paper

Nikita Borisov, Ian Goldberg, and Eric Brewer. Off-the-record communication, or, why not to use PGP. WPES 2004
Why do we need another protocol?

• A **wide variety of forms of communication** on the Internet
• Developed protections:
  – Firewalls and host security
  – Cryptography
• **E-commerce** is protected by **SSL**
• What about **social communication**?
  – **PGP** and **S/MIME** (for email)
  – **Trillian** (instant messenger)
Off-the-Record Communication

• **Private communication** over the Internet
• “We” want:
  – **Forward secrecy**
  – **Authentication**
  – **Repudiability**
• Used cryptographic primitives:
  – Perfect forward secrecy
  – Digital signatures
  – Message authentication codes (MAC)
  – Malleable encryption
Diffie-Hellman Key Exchange

Step 1: 
- $a$ is random, $A = g^a \mod p$

Step 2: 
- $b$ is random, $B = g^b \mod p$

Step 3: 
- Alice computes $K_A = B^a \mod p$
- $= (g^b \mod p)^a \mod p$
- $= g^{ab} \mod p$

Step 3: 
- Bob computes $K_B = A^b \mod p$
- $= (g^a \mod p)^b \mod p$
- $= g^{ab} \mod p$

Eve knows $A$, $B$, **not** $K$ ($K = K_A = K_B$)

System-wide **public** parameters: $p$, $g$
MACs and Malleable Encryption

- **Keyed MAC** used to verify **integrity** and **authenticity** of a message

- **MAC** is perfect for off-the-record communication. Why?
  - Provides repudiation

- **Malleable encryption** provides **forgeability**

- A message encrypted with a **stream cipher** **does not prove integrity** or **authenticity** in any way
Off-the-Record Messaging Protocol (1/2)

- **Encryption**: AES in counter mode and Diffie-Hellman key agreement

  ① $A \rightarrow B : \ g^{x_1}$

  ② $B \rightarrow A : \ g^{y_1}$

  ③ $A \rightarrow B : \ g^{x_2}, E(M_1, k_{11})$

  ④ $B \rightarrow A : \ g^{y_2}, E(M_2, k_{21})$

  ⑤ $A \rightarrow B : \ g^{x_3}, E(M_3, k_{22})$

- The protocol does not require taking turns when sending messages to each other
Off-the-Record Messaging Protocol (2/2)

- Alice must remember the old $g^{x_{n-1}}$ key until she receives a message that uses the new $g^{x_n}$ key.

- Alice generates a new key upon receiving a reply from Bob => *two own key have to be stored at a time*.

- Alice may publish an old MAC key as part of her next message.
An Implementation of Off-the-Record Messaging

• **Instant Messenger:**
  – Plugin for the popular Linux IM client GAIM (currently known as Pidgin)

• **E-mail:**
  – Ring signature can be used for email messages (extension to PGP)
  – Off-the-record protocol for every message after the first one
Related Work

• **SKME** (focused also on anonymity besides privacy)

• **Abadi’s protocol** (hides even the willingness of participates to talk to each other)

• **TESLA** broadcast authentication protocol
Conclusions

• PGP and S/MIME are useful for signing and protecting contracts or other official documents

• Off-the-record protocol is suited for social communication because it ensures forward secrecy, authentication and repudiation