Kleptographic Attacks on E-Auction Schemes

M. Gogolewski\textsuperscript{1}, M. Gomułkiewicz\textsuperscript{2}, J. Grząślewicz\textsuperscript{2}, P. Kubiak\textsuperscript{2}, M. Kutyłowski\textsuperscript{2}, A. Lauks\textsuperscript{2}

1. Faculty of Mathematics and Computer Science, Adam Mickiewicz University
2. Institute of Mathematics and Computer Science, Wrocław University of Technology

ACNS 2007, Zhuhai, China
Outline

1. Motivation
2. Kleptography
3. e-Auction Protocols
   - Harkavy, Tygar and Kikuchi’s scheme
   - Omote and Miyaji’s scheme
   - Wang and Leung’s scheme, Trevathan, Ghodosi and Read’s scheme
4. Attack
   - Types of attack
   - Example
5. Conclusions
Outline

1. Motivation
2. Kleptography
3. e-Auction Protocols
   - Harkavy, Tygar and Kikuchi’s scheme
   - Omote and Miyaji’s scheme
   - Wang and Leung’s scheme, Trevathan, Ghodosi and Read’s scheme
4. Attack
   - Types of attack
   - Example
5. Conclusions
Motivation

1. **Project:** e-Auction Platform
   - project goal – to build an integrated e-auction platform
   - team goal – to find or build a secure, trustworthy e-auction protocol

2. **Observation:** there is a lot not controlled at protocol level randomness
   - randomness opens the door to kleptographic attacks
Outline

1. Motivation
2. Kleptography
3. e-Auction Protocols
   - Harkavy, Tygar and Kikuchi’s scheme
   - Omote and Miyaji’s scheme
   - Wang and Leung’s scheme, Trevathan, Ghodosi and Read’s scheme
4. Attack
   - Types of attack
   - Example
5. Conclusions
Kleptography

- introduced by Adam Young and Moti Yung
- called - dark side of cryptography
- a technique of embedding a trapdoor in a black box cryptosystem by the manufacturer that leaks user’s private values
Kleptographic attacks – properties

- the system works according to its specification
- only manufacturer (Mallet) can get the leaking values:
  - kleptographic channel encrypted with his public key
  - the analysis of infected cryptosystem does not give access to the values send by the kleptographic channel
- possible way of detection:
  - reverse engineering - may be costly
Outline

1. Motivation
2. Kleptography
3. e-Auction Protocols
   - Harkavy, Tygar and Kikuchi’s scheme
   - Omote and Miyaji’s scheme
   - Wang and Leung’s scheme, Trevathan, Ghodosi and Read’s scheme
4. Attack
   - Types of attack
   - Example
5. Conclusions
Analyzed protocols

Harkavy, Tygar and Kikuchi’s scheme

- sealed bid auction protocol:
  - one seller, many bidders
  - bids are submitted simultaneously
  - bids should remain hidden until the bidding period is closed

Possible leak of bid values
Analyzed protocols

Omote and Miyaji’s scheme

- English auction protocol:
  - one seller, many bidders
  - bids are known to all bidders during the bidding period
  - price is pushed up by the bidders until nobody is ready to bid higher or the bidding period is closed

Possible leak of:
1. profiles of all registered users
2. secret exponents of the users (necessary for making a bid)
Analyzed protocols

Wang and Leung’s scheme, Trevathan, Ghodosi and Read’s scheme

- continuous double auction protocol:
  - many sellers, many bidders
  - bids are known during the bidding period
  - buyers and sellers submit bids for sale and purchase of a single commodity
Continuous double auctions concerned

Attack on signature schemes used in bidding process:

1. RSA – improvement of [1] – using the single elliptic curve over a prime field to key generation gives shorter key than in case of a twisted pair of elliptic curves over a binary field.

   1. all data necessary to forge the bidder’s group’s member signature
   2. profile of the bidder


Outline

1. Motivation
2. Kleptography
3. e-Auction Protocols
   - Harkavy, Tygar and Kikuchi’s scheme
   - Omote and Miyaji’s scheme
   - Wang and Leung’s scheme, Trevathan, Ghodosi and Read’s scheme
4. Attack
   - Types of attack
   - Example
5. Conclusions

A. Lauks

Kleptographic Attacks on E-Auction Schemes
Different types of attack

Software oriented attack

Assumptions:
- software does not share any individual secret with Mallet
- access to Mallet public key is required

Hardware oriented attack

Assumption:
- device and Mallet share some unique secret key $K$
- non-volatile rewritable memory
- tampered-resistant or tampered-evident device
Attack on Bidder - Omote and Miyaji’s scheme
Assumptions

- hardware attack – device contains some unique key $K$ set by Mallet
- Mallet does not have to eavesdrop any communication – he uses only publicly known values
Part of the e-auction scheme used

- to make a bid \( m_i \), the bidder \( B_i \):
  - uses \( g_{ri} \) and \( y_{ri} \) published by Auction Manager
  - must show a signature of knowledge of his/her secret exponent \( x_i \) – pair \( (c, s) \) such that:
    \[
    c = h(m_i \| y_{ri} \| g_{ri} \| (g_{ri})^s \cdot (y_{ri})^c)
    \]
    where \( h \) is a hash function
  - to determine \( (c, s) \), a bidder which knows \( x_i \) such that \( y_i = g^{x_i} \):
    - chooses at random some \( R \)
    - sets:
      \[
      c = h(m_i \| y_{ri} \| g_{ri} \| (g_{ri})^R) \\
      s = R - cx_i
      \]
Part of the e-auction scheme used

\[
c = h(m_i \| y_i^{r_i} \| g_i^{r_i} \| (g_i^{r_i})^s \cdot (y_i^{r_i})^c) \quad (1)
\]
\[
c = h(m_i \| y_i^{r_i} \| g_i^{r_i} \| (g_i^{r_i})^R) \quad (2)
\]
\[
s = R - cx_i
\]

- signature is publicly verifiable
- anyone might obtain

\[
(g_i^{r_i})^R = (g_i^{r_i})^s \cdot (y_i^{r_i})^c
\]
In the device:

- let the exponent $R$ be obtained from $\mathcal{R}(H(K))$ where:
  $\mathcal{R}$ – pseudorandom bit generator with a seed $H(K)$
  $H$ – hash function
  $K$ – some unique key set by Mallet

- After transmitting the bid the key is changed:
  $K := \tilde{H}(K)$ for $\tilde{H} \neq H$
Attack

Mallet:

1. tries to identify a device
   - gets the bid’s signature - \((c, s)\) and computes
     \[
     (g^{r_i})^R = (g^{r_i})^s \cdot (y_i^{r_i})^c
     \]
   - having a database of initial values of keys \(K\) performs series of substitutions \(K := \tilde{H}(K)\)
   - for each \(K\) gets the candidate \(R'\) for random number \(R\) and checks if \((g^{r_i})^R = (g^{r_i})^{R'}\)

2. having \(R\) gets the user’s secret exponent \(x_i\) using the equation:
   \[
   s = R - cx_i
   \]
Outline

1. Motivation
2. Kleptography
3. e-Auction Protocols
   - Harkavy, Tygar and Kikuchi’s scheme
   - Omote and Miyaji’s scheme
   - Wang and Leung’s scheme, Trevathan, Ghodosi and Read’s scheme
4. Attack
   - Types of attack
   - Example
5. Conclusions

A. Lauks
Kleptographic Attacks on E-Auction Schemes
Conclusions

- distributed trust might reduce the feasibility of kleptographic attacks

- **verifiable pseudorandomness** – output of a device should be verifiable to his owner and simultaneously completely unpredictable for others

\[ r = \mathcal{R}(\text{sig}_K(h(q))) \]

where:
- \( \mathcal{R} \) – pseudorandom bit generator
- \( \text{sig} \) – deterministic signature scheme
- \( K \) – signing key loaded to the device by its owner
- \( h \) – strong hash function
- \( q \) – unique number set by the owner
Thank you for attention