SAFE REVERSE AUCTIONS PROTOCOL
Adding Treatment Against Collusive Shill Bidding and Sniping Attacks

Ribeiro Leonardo and Guerra Ruy
Computer Center, Federal University, Recife, Pernambuco, Brazil

Keywords: Safe Reverse Auction Protocol, DSA Digital Certificate, Hash Chain, Keys Exchange, Signature Verification, Collusive Shill Bidding, Sniping.

Abstract: Many secure auction protocols were created. BJK (Byoungcheon Lee, Kwangjo Kim e Joongsoo Ma 2001) defined an efficient protocol for English auctions that can be used also for Reverse auctions. Chung (Yu Fang Chung 2008) created an improvement of BJK, however there are still some security faults that can be explored by attackers in these two protocols. In this article, we define a protocol based on BJK that is an improvement of it with the addition of security's treatment to attacks of Collusive Shill Bidding e Sniping.

1 INTRODUCTION

Internet auction is today a very popular and profitable industry. Many enterprises like Ebay, Arremate, etc; have invested in non-presence auctions. The fact that the auctions participants are not committed to be in same place brought many benefits however also many ways to cheat. There are a lot of mechanisms of cheating and many safe auctions protocols were created to solve them. These protocols were based on many cryptographic concepts like: Group Signature, Threshold Cryptography, Schnorr Signature, etc. Each solution was created to fulfill characteristics for each type of auction (English, Reverse, Sealed, etc). In this article we will present a protocol for reverse auctions. The presented protocol is based in the one proposed by BJK(Byoungcheon Lee, Kwangjo Kim e Joongsoo Ma 2001) that works very well for English and Reverse auctions. Our protocol comes to improve protocol with the use of digital certificates and a module to avoid frauds techniques known as Collusive Shill Biddings and Sniping (Trevathan, Jarrod and Read, Wayne 2006) that are not considered in any actual secure auction protocol (This protocol is being proposed to brazilian government that uses reverse auctions to buy services).

2 EXISTING PROTOCOL

The BJK protocol is one of the best already created but it still has some problems:

1. K_i keys exchange are done using Diffie-Hellman without authentication which enables ”Man in the Middle” attack.
2. It uses Schnorr signature for authentication of bidder that is not very used in commercial certificates(RSA and DSA are the most used).
3. It does not consider attacks like Shill Bidding and Sniping.

We propose a protocol wich is an improvement of BJK where:

1. All auction's bidders will use DSA digital certificates for authentication.
2. The keys exchange using Diffie-Hellman will be done using DSA certificates for authentication with bidder doing this exchange with Auctionner through Register Manager(RM).
3. A fraud module(FM) will implement Shill Bidding detection.
4. Anti Sniping policies will be implemented by RM.

2.1 Our Protocol

2.1.1 Phases

1. Registration
   (a) B_i has a private key x_i and a public key y_i defined in his DSA digital certificate.

Ruy G. and Leonardo R. (2009).
SAFE REVERSE AUCTIONS PROTOCOL - Adding Treatment Against Collusive Shill Bidding and Sniping Attacks.
In *Proceedings of the International Conference on Security and Cryptography*, pages 239-244
DOI: 10.5220/0002228902390244

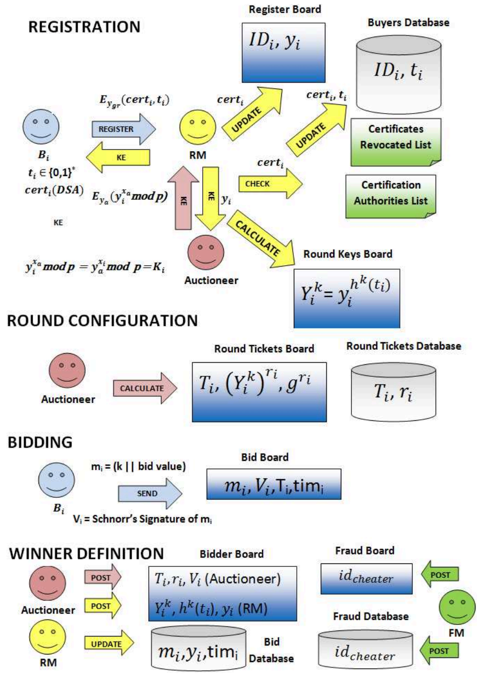

Figure 1: Protocol Phases Representation.

(b) B_i registers in auction connecting to RM using his certificate to create a SSL conection with mutual authentication. The certificate is verified against CAs database. It's verified the validation of certificate's expiration date and if it's in list of revocated certificates of the cerficate's CAs. I't also verified if bidder id and/or public key are in the list of mean bidders.

(c) After B_i is authenticated, he/she chooses a random string $t_i \in \{0,1\}^*$, keeping it safely by encripting it whith his private key defined in his digital certificate.

(d) B_i sends t_i and his certificate $cert_i$ to RM encripting them with RM's public key.

(e) RM decripts data and publish (ID_i, y_i) in "Registration" board where ID_i comes from digital certificate(See picture above). RM keeps (ID_i, t_i) secretly in bidders database.

(f) RM calculates round key as: $Y_i^k = y_i^{h^k(t_i)}$ for all n valid bidders.

(g) RM publishes them in "Round Keys" board.

(h) RM sends y_i to auctioneer and ask him to generate $y_i^{x_a}$ mod p.

(i) The auctioneer calculates $y_i^{x_a}$ mod p, encrypt it with RM's public key and send it back to RM.

(j) RM receives data and decrypts it, send $y_i^{x_a}$ mod p to B_i encrypting it with his public key.

(k) B_i receives $y_i^{x_a}$ mod p , decrypts it and stores it localy encrypts it using El Gamal algorithm.

Remember that $K_i = y_i^{x_a} = y_a^{x_i}$ defined by Diffie-Hellman key exchange algorithm.

Remarks:
The bidder B_i can verify if his round key is in "Round Keys" board.
No one except RM and B_i know the correspondence of y_i and (Y_i^k).

2. Round Configuration

(a) Auctioneer takes the list of round keys (Y_i^k) from "Round Keys" board.

(b) Auctioneer generates n random numbers $r_1, ..., r_n \in Z_q$ for each valid bidder where q is retrieved from public key of Auctionner certificate (Rembering that g, p and q are the same for all certificates of entities participating in auction).

(c) Auctioneer calculates $((Y_i^k)^{r_i}, g_i^{r_i})$ where k is the number of round, g is retrieved from public key of Auctionner certificate and r_i is the random number defined as above for each bidder B_i.

(d) Auctioneer calculates round ticket as $T_i = h((Y_i^k)^{x_a})$ where x_a is auctioneer's private key.

(e) Auctioneer publishes round ticket $(T_i, (Y_i^k)^{r_i}, g^{r_i})$ on "Round Tickets" board.

(f) Auctioneer stores (T_i, r_i) secretly in "Round Tickets" database.

Remarks:
The Auctioneer does not know the correspondence of y_i and (Y_i^k) as RM does not know from T_i and r_i.
See that a bidder can verify round ticket T_i calculating:
Let $K_i = y_i^{x_a} = y_a^{x_i}$ like defined in registration phase and $(T_i, (Y_i^k)^{r_i}, g^{r_i})$
Then
$T_i = h((Y_i^k)^{x_a}) = h((y_i^{h^k(t_i)})^{x_a}) = h((y_i^{x_a})^{h^k(t_i)}) = h((y_a^{x_i})^{h^k(t_i)}) = h(K_i^{h^k(t_i)})$ and this value can be calculated by B_i because he/she has K_i and t_i and he/she knows how to calculate $h^k(t_i)$.

3. Bidding
The bidder B_i that wants to participate in round k of auction must follow the steps defined below while the auction's round has not expired:

(a) Calculates his round key $Y_i^K = y_i^{h^k(t_i)}$ and verifies if it's in "Round Keys" board defined by RM.

(b) Calculates $T_i = (h(y_a^{h^k(t_i)}))^{x_i}$ and takes his ticket $(T_i, (Y_i^k)^{r_i}, g^{r_i})$ in "Round Tickets" board.

(c) Verifies the ticket through $((g^{r_i})^{h^k(t_i)})^{x_i} =? (Y_i^k)^{r_i}$. If there's a problem, tell Auctioneer.

(d) Prepares his bid (T_i, m_i, V_i) as defined below:

  i. $m_i =$ (auction's round number || bid's value)

  ii. Signs m_i with Schnorr's Signature of Knowledge to assure anonymity: $V_i = (c, s)$ where $c = h(m_i||(Y_i^k)^{r_i}||g^{r_i}||(g^{r_i})^{k_i})$, $s = z_i - c.h^k(t_i)x_i \mod q$ and $z_i \in Z_q$.

(e) B_i updates "Bids" board with (T_i, V_i, m_i). It's stored the tuple (T_i, V_i, m_i, tim_i) where tim_i is the time of bidding."Bids" board verifies if bid value is lower than current for V_i. No one except the bidders can update "Bids" board.

(f) RM controls the round's auction time. He verifies the rate of bids per minute in auction's round based on changes of "Bids" board. If there's an anormal rise of bids in round's last 2 minutes, time is extended more x minutes (x is a parameter defined in auction's round beginning), avoiding this way Sniping attack.

Remarks:
Note that V_i can be verified by anyone that knows r_j, $h^k(t_j)$ and Y_j^k according to Schnorr's signature of knowledge $c? = h(m_i||(Y_i^k)^{r_i}||g^{r_i}||(g^{r_i})^s((Y_i^k)^{r_i})^c)$.

4. Winner Definition

(a) After auction's round has finished, RM and Auctionner take the lists of "Bids", "Round Keys" and "Round Tickets" boards and find bidders identities following the steps:

  i. Auctionner takes $(V_j, m_j, T_j, time_j)$ from "Bids" board.

  ii. Auctionner posts (T_j, r_j, Y_j^k) on "Bidders" board that reveals the correspondence of Y_j^k and $(Y_j^k)^{r_j}$. Bidder's information becomes (V_j, T_j, r_j).

  iii. RM posts $(Y_j^k, h^k(t_j), y_j)$ on "Bidders" board that reveals the correspondence of $Y_j^K = y_j^{h^k(t_j)}$ and y_j. Bidder's information becomes $(V_j, T_j, r_j, Y_j^k, h^k(t_j), y_j)$.

  iv. RM updates "Bids" database with m_i, bidder's public key y_j and tim_j.

  v. Anybody can verify the bidder's signature V_j using the announced public values r_j, $h^k(t_j)$ and (Y_j^k).

(b) Fraud module verifies the existence of "Collusive Shill Bidding"(See next section for more explanations) based on "Bids" database. If it's found a collusive shill bidding, the auction's round is invalidated and bidders found to be cheating are included in "Fraud" board and in "Fraud" database.

(c) If no frauds were found, the bidder with lowest bid value is announced as winner.

3 FRAUD MODULE

3.1 Shill Bidding

3.1.1 Introduction

Jarrod Trevathan and Wayne Read (Trevathan, Jarrod and Read, Wayne 2005) proposed an algorithm for Shill Bidding Detection of only one shill. After, the same authors proposed an improvement of this algorithm for the case of a shill with more than one bidder, also known as Collusive Shill Bidding (Trevathan, Jarrod and Read, Wayne 2007). We are going to use this last algorithm to propose a module that can be used in our protocol for detecting collusive shill bidding. This algorithm doesn't run on real time but after an auction is finished. The algorithm, based in ratings, calculates what is called shill score. The score informs if a specific bidder is working with others to form a collusive shill bidding. Based on this score, an auction can be invalidated and bidders are denied to participate in more auction's rounds. The detection of a shill is based in calculation of these ratings:

1. α: Percentage of auction's rounds a bidder i has participated.
2. β: Percentage of bids that bidder i has submitted throughout all the auction's rounds he/she has participated in.
3. γ: How many times the bidder has won over the auction's rounds he participated in.
4. δ: The average inter bid time of bidder in the auction's rounds he participated in.
5. ε: The average inter bid increments in the auction's rounds he participated in.
6. ζ: indicates how early in an auction's round bidder i started bidding.

These ratings are defined in interval $(0, 1)$. The higher values, more suspicious the bidder is. If zero values, bidder has won the auction.

Based on these ratings, we can calculate a shill score for one bidder as:
$SS = ((\theta_1\alpha + \theta_2\beta + \theta_3\gamma + \theta_4\delta + \theta_5\varepsilon + \theta_6\zeta)/(\theta_1 + \theta_2 + \theta_3 + \theta_4 + \theta_5 + \theta_6)) \times 10$ where $1 \leq \theta_i \leq 6$

For the case of Collusive Shill Bidding, there are more than one bidder working together and the calculation of these ratings and their scores doesn't imply that the bidders are in an agreement. Only using these parameters to detect shills can include legitimate bidders. Then, other techniques should be used. There are three ways a collusive shill bidding act and we can create mechanisms to detect them.

3.1.2 Forms of Collusive Shill Bidding

1. Alternating bids: Shills (a shill is a bidder that participates in a collusive Shill Bidding) bid in only one auction's round to increase or decrease the price.
2. Alternating rounds: Bidders take turns bidding as a collusive shill in different auction's rounds with one shill per round.
3. Hybrid: Bidders take turns bidding as a collusive shill in more than one auction's round simultaneously.

3.1.3 Detection Mechanisms using Graphs

Collusion Graph

To detect the collusive shill biddings, it's defined the concept of Collusion Graphs. A collusion graph is defined as G=(V,E) where V is the set of bidders and E is the edges between them. Each edge $e_{i,j}$ exists if they participated in a same auction's round. Each edge has a weight w_i that defines the number of times two bidders v_i and v_j participated in same auction's round. If the two bidders participated together in only one auction's round, $w_i = 0$ and $w_i >= 1$ otherwise. Each edge has a weight w_i, $1 <= i <= l$, where l is the number of bidders, that defines the number of times two bidders v_i and v_j participated in more than one auction's round together.(See example on figure 2 below).

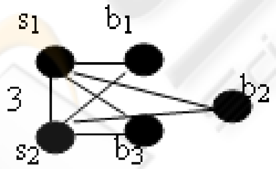

Figure 2: Collusiong Graph Normalization.

The graph above was generated for the sequence: $(s_1, b_1, s_2, b_1, s_1, b_1)$ for first auction's round, (s_2, b_2, s_1, b_2) for second auction's round and $(s_2, b_3, s_1, b_3, s_2, b_3)$ for third auction's round (s_i means shill i and b_i bidder i). Based in the Collusion Graph, it's calculated a collusion rating for each bidder v_i as:

$n_i^{'} = \sum_j^k w_j$ where k means the degree of bidder i in graph and $1 <= j <= l$ where l is the number of bidders.

Each bidder collusion rating is normalized as:

$n_j^{'} = \frac{(n_i^{'} - n_{min})}{(n_{max} - n_{min})}$ where n_{min} is the lowest value of all values $n_i^{'}$ and n_{max} the highest.

According to $n_j^{'}$ normalized values, suspicious bidders are separated as sets denoted by C_k and $C = \{C_1, C_2, C_3, ., C_k\}$ is the set of bidders grouped by $n_j^{'}$. If two bidders, b_i and b_j, are suspicious and they have similar collusion rate, i.e., $n_j^{'} = n_i^{'} + \lambda$ where λ is an error factor, they will be in a same collusion set. Bidders not suspicious will be in a set of one element. See that $1 <= k <= l$ where l is the total number of bidders. The $n_j^{'}$ values are then used to join suspicious in a same set and preserve the correct bidders.

The collusion graph is used in Alternating bids form.

Dual Graph

It's a graph used in Alternating rounds form. It's the opposite of Collusion graph. In this graph, two nodes are connected if they didn't participate in same auction's round. In this graph, we are not interested in the quantity of how many auctions they participated but in if they weren't cooperating or not in same round. So weight information has value one(1) if there's cooperation and zero(0) if not.In example with auction's round one sequence as (s_1, b_1, s_1, b_2) and auction's round sequence two as (s_2, b_1, s_2, b_2), it can be defined a Collusion graph as figure 3 and a Dual graph as figure 4.

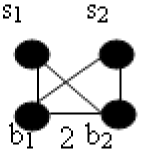

Figure 3: Collusion Graph.

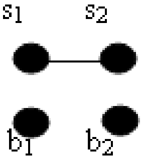

Figure 4: Correspondent Dual Graph.

Based in the Dual Graph, it's calculated a collusion rating for each bidder v_i as:

$\theta_i^{'} = \sum_j^k w_j$ where k means the degree of bidder i in graph and $1 <= j <= l$ where l is the number of bidders.

Each bidder collusion rating is normalized as:

$\theta_j{'} = \frac{(\theta_i^{'} - \theta^{min})}{(\theta^{max} - \theta^{min})}$ where θ^{min} is the lowest value of all values θ'_i and θ^{max} the highest.

According to θ'_j values, bidders are separated as sets denoted by C^θ_k and $C^\theta = \{C^\theta_1, C^\theta_2, C^\theta_3, .., C^\theta_k\}$ is the set of bidders grouped by θ'_j. If two bidders, b_i and b_j, are suspicious and they have similar collusion rate, i.e., $\theta'_i = \theta'_j + \lambda$ where λ is an error factor, they will be in a same collusion set. Bidders not suspicious will be in a set of one element. See that $1 <= k <= l$ where l is the total number of bidders.

The dual graph is used in Alternating rounds form.

3.1.4 Alternating Bids

Bidders with similar collusion ratings defined by collusion graph will have high probability to be in a same shill. However this parameter isn't enough to define that a bidder belongs to a shill. It's observed that shill bidders in alternating bids have identical β ratings. Based on that, a variable called bidding factor is defined as:

$$\begin{aligned} \phi^\beta_{i,j} = 1 \quad & if \quad \beta_i = \beta_j \\ \frac{\beta_i}{\beta_j} \quad & if \quad \beta_i < \beta_j \\ \frac{\beta_j}{\beta_i} \quad & if \quad \beta_i \geq \beta_j \end{aligned}$$

It defines how similar two bidders are for this type of collusive shill.

The parameters n'_i, $\phi^\beta_{i,j}$, γ, δ and ε are then combined together to define a new parameter called Collusion Score.

$CS^n_i = (\frac{(\gamma+\delta+\varepsilon+n'_j+\phi^\beta_\sigma)}{5}) \times 10$, where ϕ^β_σ is the average of all $\phi^\beta_{i,j}$.

For each set C_k that is not singleton, it is calculated bidder's collusion score and bidders with similar collusion score will be defined as bidders of a same shill.

3.1.5 Alternating Rounds

In alternating rounds, as in alternating bids, we can define collusive bidders based on parameter Collusion Score. However to calculate it, we observe a different characteristic. It's observed that shill bidders in alternating rounds have identical α ratings. Based on that, the bidding factor is defined as:

$$\begin{aligned} \phi^\alpha_{i,j} = 1 \quad & if \quad \alpha_i = \alpha_j \\ \frac{\alpha_i}{\alpha_j} \quad & if \quad \alpha_i < \alpha_j \\ \frac{\alpha_j}{\alpha_i} \quad & if \quad \alpha_i \geq \alpha_j \end{aligned}$$

It defines how similar two bidders are for this type of collusive shill.

These parameters θ'_i, $\phi^\alpha_{i,j}$, ζ, δ and ε are then combined together to define a new parameter called Collusion Score.

$CS^n_i = (\frac{(\zeta+\delta+\varepsilon+\theta'_j+\phi^\alpha_\sigma)}{5}) \times 10$, where ϕ^α_σ is the average of all $\phi^\alpha_{i,j}$.

For each set C^θ_k that is not singleton, it is calculated bidder's collusion score and bidders with similar collusion score will be defined as bidders of a same shill.

3.1.6 Hybrid

The hybrid's form combines the alternating bids and alternating rounds form. It uses both graphs for detection of shills. It uses the Collusion Score as:

$CS^h_i = (\frac{(\delta+\varepsilon+\eta+\phi^\beta_\sigma+\phi^\alpha_\sigma)}{5}) \times 10$, where ϕ^β_σ and ϕ^β_σ are calculated for alternating bids and rounds forms like already defined in the last sections.

3.2 Sniping

To avoid sniping in an auction, it should be followed policies to avoid them. The most used technique to avoid it is to extend auction time if there are bids sent in the last minutes. In this paper, as defined in Bidding phase of protocol, the auction is extended x minutes if there are bids sent in the last 2 minutes (x is a parameter defined by auctineer). It avoids bids run in the last minutes. Sniping is a very known technique used by bidders in the most popular auctions of internet like Ebay, etc; but this behavior of bidders is not accepted because it does not allows the real English(Reverse) auction process of price increasing(or decreasing) in a period of time. Sniping transforms English(Reverse) auction in a sealed auction because almost all the bidders bid at the very end of auction's round time with each one sending a sealed letter at the same time.

4 ANALYSIS

4.1 Protocol

1. Anonym bidder: The RM cannot know the bidders from $(Ti, (Y^k_j)^{r_j}, g^{r_i})$ and (T_i, m_i, V_i) because

know Y_j^k and $(Y_j^k)^{r_j}$ is a problem of calculation discrete logarithm. Without K_i, RM does not know T_i and find V_i is also a discrete logarithm problem. The auctioneer has no knowledge of Y_j^k from $(Y_j^k)^{r_j}$ and also does not know V_i.

2. Publicly Verifiable: With RM and auctioneer data, B_i winner can be verified.
3. Bids not Forgeable: RM, the auctioneer and anyone cannot forge the signature V_i of bidder B_i.
4. No repudiate: The B_i winner cannot refuse his bid because it's signed with V_i.
5. Efficiency:

(a) The bidder registration: takes one generation of signature and a verification of signature through SSL authentication(1SG + 1SV). One encryption for sending certificate and t_i values, two encryptions and decryptions for Diffie-Hellman exchange with authentication(Bidder, RM and Auctioneer communication).

(b) Round key generation takes a modular exponentiation (1E).

(c) Auction ticket generation takes three modular exponentiations (3E).

(d) The bid sending takes two modular exponentiations and a signature generation (2E + 1SG).

(e) The winner's definition takes two modular exponentiations and one signature verification (2E + 1SV) for each bidder.

(f) Module fraud detection cost: Construction of Collusive graph using adjacency lists to build an adjacency matrix + scan adjacency matrix($O(n)$) + calculation of shill's rates ($O(n)$) + calculation of collusion rates ($O(n)$) + construction of collusive rate sets($O(1)$) + calculation of collusive score ($O(n)$).

4.1.1 Sniping

There are not cost associated to this part of module because the techniques to avoid Sniping are very simple according to section above.

5 CONCLUSIONS

It's already known the efficiency of BJK protocol for English auctions, but it does not consider none cryptographic attacks. Our protocol intends to improve BJK's one adding techniques for treatment of Collusive Shill Bidding and Sniping attacks.It also adds authentication through DSA digital certificates. Our protocol is built in a such form to protect reverse auctions against these forms of attacks.

We are simulating all protocol to prove his efficiency with real data. We are also trying to implement improvements like the ones proposed by Chung.

ACKNOWLEDGEMENTS

To professor Ruy Guerra to all his help and advices. Following always the idea to never give up.

REFERENCES

Trevathan, Jarrod and Read, Wayne (2006). *Undesirable And Fraudulent Behaviour In Online Auctions In Security and Cryptography Conference (SECRYPT), 450 458*

Byoungcheon Lee, Kwangjo Kim e Joongsoo Ma (2001). *Efficient Public Auction with One-time Registration and Public Verifiability*. In *Second International Conference on Cryptology in India, Indocrypt'01, 162-174, Springer-Verlag, LNCS 2247*

Trevathan, Jarrod and Read, Wayne (2005). *Detecting Shill Bidding in Online English Auctions*. Technical Report, 2005. Available at http://auction.maths.jcu.edu.au/research/shill.pdf

Trevathan, Jarrod and Read, Wayne (2007). *Detecting Collusive Shill Bidding*. In International Conference on Information Technology – ITNG'07, page 799-808 Jame Cook University, North Queensland , Australia.

Yu Fang Chung 2008. *Bidder-anonymous English Auction Scheme with privacy and public verifiability*. In *Science Direct, The Journal of Systems and Software 81, 2008, 113-119.*