ON SECURE E-VOTING SYSTEM USING DIAMETER BASE PROTOCOL

Anil Pandit 1, R. C. Gangwar 2

1Research Scholar, I.K.G.Punjab Technical University, Kapurthala, Punjab, India.
2Associate Prof. ,Dept. of Computer Sc. & Engg, Beant College of Engineering & Technology, Gurdaspur, Punjab, India.

ABSTRACT:

We propose a Diameter based electronic voting protocol that attempts to achieve the authentication, authorization, accountability, security of ballots and privacy of voters using a cryptographic method. Our paper fundamentally proposes an E-Voting system, which uses internet network for voting a particular candidate in the election process. For security of E-Voting process over the network we propose the implementation of a Diameter protocol in E-Voting. The e-voting procedure is easy and it needs only selecting the intention of voter over the screen of any electronic device. Increase of Internet Network, online electronic voting is a reasonable alternative to electronic voting machines and other opinion using conventional voting kiosk or voting processes. Current research focuses on implementing and using of Diameter based triple AAA “voting protocols” which supports the secure e-voting process, while implementing the security instruments required for preventing deception and defending voter's privacy. Diameter protocol is a peer-to-peer protocol, and also a Diameter protocol servers can ask for certain important services. This protocol uses either SCTP (Stream Control Transmission Protocol) or TCP (Transmission Control Protocol). This protocol’s process is more consistent, primarily because its description discourses issues e.g. fail-over procedure and proxy/agent support. Possible “security gaps” in the managerial or user workflow may result in worsening the overall security level of the system, but if the strong AAA based voting protocol implemented by the e-voting system succeeds to fully comply with the security necessities set for e-voting. To this course, this paper terms the importance of the protocol and introduces the new Diameter based triple AAA protocol in the electronic voting process.
ON SECURE E-VOTING SYSTEM USING DIAMETER BASE PROTOCOL

Keywords : E-Voting, Diameter, EVM’s, Cryptography, SCTP, TCP, AAA, Radius

[1] INTRODUCTION

Secure electronic voting systems over Internet, is a prime requirement of a modern autonomous societies. It can easily stop or detect scams , and so deliver precise outcomes. To escalate transparency in such system, researchers have been designing secure voting schemes. To increase the voter turnout in any democratic country , one should implement the internet based e-voting and reach to every individual voter for voting through any electronic device. These schemes allow the voters to cast their votes securely by using authentication methods. This paper presents Diameter based protocol which is inherited from the RADIUS protocol with multiple enhancements in different aspects, and is the following generation Verification, Authorization, and Bookkeeping protocol also known as AAA protocol. This article presents a proposal that address the security of three important properties, Authentication , Authorization and Accountability using cryptographic methods to send encrypted votes to the Server. E-voting which through new machineries and new requests such as wireless nets and portable devices, the importance of authentication and authorization have significantly improved, and access control mechanisms are more compound than forever. RADIUS (Remote Authentication Dial-In User Service) protocol is inadequate to fulfil new necessities; a fresh new protocol is required which is accomplished of satisfying new access control structures while keeping the elasticity for further delay.

Most eligible voters joining in voting process, during elections must the choice of casting ballots using a web browser over the Internet. Canada, Estonia, France and Switzerland are some countries, which use voting through electronic means. These are just a rare examples of increasing drift towards Internet network established voting. Though voting of this kind appears to inspire upper voter turnout and make accurate accounting for votes stress-free, it also carries the potential of making abuse easier to perform, and at a large scale. A slew of documents in the cryptographic literature have described ways of achieving robust and authenticated automatic elections. This paper introduces Diameter - based Protocol in E-Voting in which a voter can be authenticated, authorized in a modest, but well-organized way to bring such AAA competence. Voter votes through any electronic device using a valid ID/ username & password and then he could be authenticated through Diameter based protocol, which includes failover, security, and auditability. Diameter-based protocol checks all aspects of AAA including error handling and message delivery reliability. Diameter based e-voting protocol is planned as a peer-to-peer design, and each electronic device which implements the Diameter-based procedure can act as either a client or a server depending on network deployment in e-voting architecture system by the election officials. So the term Diameter node is used to refer to a Diameter e-voting client, a Diameter voting server, or a Diameter e-voting agent, that will be introduced later in this paper. The Diameter e-voting node that receives the e-voter user connection request will act as the Diameter e-voting client. In most cases, a Diameter e-voting client will be a Network e-voting Access Server. After collecting user credentials, such as username and password, it will send an access request message to one Diameter e-voting node serving the request. The Diameter e-voting node /server authenticates e-voter based on the information provided. If the authentication process succeeds, the e-voter’s access privileges are included in the response message and sent back to the corresponding Diameter e-voting client, else, an access reject message is sent. If
successful then Diameter protocol checks for authorization that can check an e-voter can vote or not; and also checks the credentials of a valid e-voter to use the resources. Auditability in Diameter protocol can check for how much time a user can logs into the website of election commission and what the e-voter did. Although the e-voting design just described seems an outdated e-voting client-server architecture, a node acting as the Diameter e-voting server for some requests might actually act as a Diameter e-voting client in some situations, the Diameter protocol is actually peer-to-peer-based architecture in a more generic sense. Besides, a special Diameter node called Diameter e-voting agent is obviously well-defined in Diameter protocol. This makes e-voting election procedure to be secure against a variety of fraudulent behaviours.

[2] REVIEW OF LITERATURE

In [1], Fujioka, Atsushi et. al has ensured fairness for voters while participants in this scheme are voters, administrator and a counter. The scheme presented safeguards the confidentiality of the voters even if both the supervisor and a counter collude and realizes voting fairness. It also ensures the privacy and prevents any disruption by voters or the administrator.

In [2], David Chaum et al. derived a new type of cryptography namely Blind Signatures, where in Verifiability could be checked without breaching the privacy of an individual Voter.

In [3], Jefferson, David et. al. proposed a Secure Electronic Registration and Voting Experiment (SERVE) which is an Internet based voting system built by Accenture and its subcontractors for the U.S. Department of Defence. Various researchers exposed the vulnerabilities of SERVE, which was dangerous for Internet voting (SERVE) as Internet is independent of national boundaries, an election held over the Internet is vulnerable to attacks from anywhere in the world. Not only could a political party attempt to manipulate an election by attacking SERVE, but so could individual hackers, criminals, terrorists, and even other rogue countries. Lack of voter-verified audit trail and insider assaults, denial of service attacks, tricking, automated vote buying, virus-related attacks on voter PCs, etc., may be catastrophic.

In [6], Wolchok, Scott et. al. evaluated the EVMs used in Indian elections and practically examined these devices. These have been praised for their simple design, easy to use by the voter, and reliability, but they have also been problematic following widespread reports of election irregularities. This paper presents a security analysis of a real Indian EVM obtained from an anonymous source. The machine’s design and operation in detail are susceptible to serious attacks that can alter election results and violate the secrecy of the ballot. This paper gives an important lesson to ECI on electronic voting security more generally. Secrecy and Voter’s faith cannot be proved using EVMs.

Christopher Metz. explained the Diameter protocol as an AAA protocol which is intended as an enhanced Variety as well as substitute of RADIUS Protocol. Diameter Protocol adds up more capability for the advancement of Security design for Distributed Network System in order to track which services and resources used. Authorization and Accounting in cloud based
environment as well as its applications have significant role because of support of huge seamless enterprise coverage with globalized communities of subscribers. This paper have presented an overview on how recent and advanced features have evolved with the application of Diameter based protocol in New and Imminent Technologies.

Hosia et. al. [9] presented the difference between two protocols RADIUS and Diameter, RADIUS is a broadly installed protocol for Authentication, Authorization, and Accounting control, while Diameter is a draft planned as its successor. The protocols look alike each other in many methods, for example, their packet formats are quite alike, and they provide support for same kind of AAA mechanisms. However, while RADIUS is a pure client-server protocol, Diameter is more of a peer-to-peer protocol, as also Diameter servers can ask for certain services. On the transport layer RADIUS uses connectionless UDP protocol, while Diameter uses either SCTP or TCP protocol. Diameter’s operation is more dependable, mainly because its specification addresses issues such as fail-over procedure and proxy/agent support, while RADIUS design neglects these subjects.

[3] THEORETICAL FRAMEWORK

After going through literature review, it has been found that Diameter protocol is the best suited protocol for secure electronic voting. The Diameter protocol is an improved version of Radius Protocol for Authentication, Authorisation and Accountability, as its name references, is a new RADIUS rules. It comprises ample improvements in all parts, such as error management and message transfer consistency including various novel methods. Diameter protocol inherits the essence of the triple A protocol from RADIUS which defines a group of messages that are overall and simple enough to be the primary base for Voting protocol using the Diameter Base protocol. Many applications which require triple A functions can define their own new additions to the Diameter rules, and can profit from the fundamental skills provided by the Diameter base rules. Figure 1 below exemplifies the affiliation between the Diameter base rules and various Diameter based applications.

![Figure 1. The bond of the Diameter base protocol and Diameter based applications](image-url)
[4] METHODOLOGY

As our methodology is typically using the Diameter based protocol, Fig. 2 below shows the working of different layers in a TCP/IP model.

![Layers for Diameter Protocol Based Application](image)

**Figure: 2.** TCP/IP Model using Diameter based protocol at application layer.

**The Actors and their roles:**

Our system is designed for on-line E-Voting. Every E-voter possesses an voting Id Number and password that are used to vote on online voting system. Our system involves several peer to peer voting clients / voting servers. A voter logs into the system using this credentials through a Point-to-Point protocol to access the resources of e-voting website portal. Figure 3 depicts the working of the system as the voter logs into the system.

As our focus is on Authentication and Authorization, the Diameter protocol is not specific to only one application which works on uppermost of the layer. It emphasizes on common message swapping structures between voter and the voting server using Diameter protocol. Because authentication and authorization practices are different among applications, the Diameter base protocol are without command codes and AVPs (attribute value pairs) used primarily in authentication and authorization. Here it is mentioned that AVPs are the data structure used to modify or delete the fields and used to design the data structure of the of the e-voting system. It is necessary for the Diameter e-voting applications to define their own messages and corresponding attributes based on the e-voting application's characteristics. For example, the Authentication and Authorization request by the e-voter / administrator message is used to carry out authentication and authorization information in the V-NAS(Voting Network Access Server) application, while in the E-Voting application the message could be called as a Voter-Authorization-Request.
Accounting
Not only verification and authorization but, the behaviour and the message to be exchanged for bookkeeping message is evidently defined. Bookkeeping in Diameter protocol essentially monitors a server focused model, which means that any node or device that generates accounting records monitors the direction of an authorization server.

Based on the voter profile, a Diameter Voter server informs the corresponding Diameter Voter client as to what behaviour is expected, such as how often the accounting record should be sent from Voting client to Voting server, or if the voting bookkeeping record should be generated continuously and it should be within an accounting session.

Depending on the service to be provided, there are two kinds of voter accounting records: For one-time invocation-based services, the VOTER_EVENT_RECORD is used. However, if the service will be provided in a measurable period, the accounting record types VOTER_START_RECORD, VOTER_INTERIM_RECORD, and VOTER_STOP_RECORD could be used to mark the start, update, and end of a session of an e-voter.

To stop replicated voter bookkeeping records, each voter accounting message is associated with a voter Session-Id AVP (Attribute value Pairs) along with a Voter-Accounting-Record-Number V-AVP. As this combination can distinctively identify an accounting record of a e-voter, a Diameter voting node acting as a Diameter voting agent can use this information to detect repeated accounting messages being sent to the Diameter voting server, thereby evading unnecessary processing for the Diameter based voting server. This situation might come from short-term network problems or voter client shutdowns. Also, it is required that the Diameter voting user keep a local reserve of outgoing voter accounting messages until a voter acknowledgement message arrives.

Error management
Errors in the Diameter fall into two classes: procedure errors and e-voting application errors. Procedure errors denote to something being incorrect with the essential protocol used to carry Diameter messages, perhaps incorrect routing information or temporary network failure. E-Voting Applications errors, on the other hand, result from the failure of the Diameter protocol itself, and there are slew of sources that will cause application errors. For example, when a mandatory Voting AVP is missing in a particular Diameter command, a DIAMETER_MISSING_AVP error code is returned. Every response message in Diameter will carry a Result-Code AVP, and the receiver of a response message can check this Voting AVP to see if the previous message was successfully processed. To upkeep early connection failure discovery, the Diameter protocol defined a Device-Watchdog-Request message. When two connected Diameter based voting nodes/devices don't exchange messages for a certain length of time, this message is sent from either of these voting nodes/devices to detect possible network glitches/errors. The discussion of algorithms to detect transport failures is beyond the scope of this paper. The Diameter protocol shares the same semantics of error code definition as the HTTP protocol. The return status of messages can be easily identified by checking the first digit of the return code:

1. 1xxx: means the request can't be satisfied and extra information is mandatory for the service to be approved.
2. 2xxx: means the request was processed fruitfully.
3. 3xxx: means there was a protocol error when transmitting a Diameter message. Generally, a Diameter proxy should try to fix this problem by either routing the message to another Diameter server, or by keeping the message in a local cache and sending it again later.
4. 4xxx: means the requested message cannot be satisfied at the moment, but it might work in the future. An example is a server that temporarily lacks physical storage space to handle any incoming requests.

5. 5xxx: means that there was an application error as the server was processing the request message. The sender should not try to send the same message again. Instead, the sender will have to determine the cause of the application error by checking the error code, and then fix the problem.

Besides the Return-Code AVP, the message sender can also check other Voting AVPs that carry additional information for error handling. The Error-Message AVP carries human readable error messages and can be used to determine the actual cause. The Error-Reporting-Host AVP contains the identity of the host generating the Result-Code. This AVP is very helpful for troubleshooting to spot the location of a problem. The Failed-AVP contains the group of AVPs that caused the exception. After an error has been detected, the sending node forwards all pending messages to an alternative Diameter node. This process is called Fail Over. A pending message is a message that has been sent, but hasn't received its corresponding answer yet. It is required for each Diameter rules based node/device to keep a record of its outgoing data. The node-to-node Identification within each protocol data unit is used to reference which are out communications for each target peer. However, this process may cause a Diameter based node to receive an same message more than one time. The Diameter protocol Voting node/device must use the combination of first device to last device Identification message header and Original -Voting Host AVP to uniquely recognize a message coming from a exact Diameter voting node.

[5] DIAMETER BASED VOTING AGENTS

Voting Relay Agent
A Voting Relay Agent is used to advancing a voting message to the suitable destination, but it only depends on the message or information in the message. The Voting Relay Agent is useful because it can aggregate requests from different territories (or regions) to a specific territory, which eliminates the difficult configurations of voting network access servers for every Diameter based Voting server change.

Proxy Voting Agent
A Proxy Voting Agent is being used to deliver the forward messages, but contrast to a Voting Relay Agent, a Proxy Voting Agent can change the message content and will provide many services which are mainly value-based, enforce rules on different messages, or perform directorial jobs for a precise domain. Figure 4 shows how a Proxy Voting Agent is used to send and advancing a message to another domain using an example.com site. If the Proxy

![Figure: 4. The Diameter Proxy Voting Agent](image-url)
Voting Agent will not modify the content of an original request, a Voting Relay Agent in this scenario would be sufficient.

Redirect Voting Agent
A Redirect Voting Agent acts as a integrated formation depository for additional Diameter voting nodes. When it receives a voting message, it checks its voter routing table, and returns a response message along with redirection information to its original voting sender. This would be very convenient for other Diameter based nodes/devices because they do not keep a list of routing entries in the neighbourhood and can look up a Redirect Agent when needed. Figure 5 exemplifies how a Redirect Agent works. The scenario in Figure 3 below is basically matching to the one in Figure 4, but this time the Proxy Voting Agent is not aware of the address of the contacting Diameter voting node inside example.com. At last it looks up the evidence in the Redirect Agent of its own territory to get the statement.

![Diagram of Diameter Redirect Voting Agent](image)

**Figure: 5. The Diameter Redirect Voting Agent**

Translation Voting Agent
In tally to these proxies, there is a one more voting agent called Translation Voting Proxy. The accountability of this agent, is to change a voting message from one AAA procedure to another. The Translation Voting Agent is helpful for the election officials to integrate the voter database of two application domains, though keeping their original AAA procedures. Another condition is that a voter wants to transfer to Diameter protocol, but the movement consists of many stages. The Translation Voting Agent could provide the backward ability for an easy migration. Figure 6 shows how one agent translates the RADIUS protocol into the Diameter protocol, but, of course, other kinds of procedure translation (for example, Diameter to RADIUS, Diameter to TACACS+) are also possible.

![Diagram of Diameter protocol Translation Agent](image)

**Figure: 6. The Diameter protocol Translation Agent**

Anil Pandit and R. C. Gangwar
[6] CONCLUSION

In this paper a new authentication, authorization and accounting e-voting system using Diameter protocol is presented wherein it is showing how different agents in the Diameter protocol works together to achieve the specified goals. Many characteristics, including its role and obligation of different Diameter protocol based devices/nodes, the structure of a Diameter message, and how communications are sent and received and how triple AAA and error handling are achieved in Diameter based voting protocol. We have to develop and implement as how the Diameter based voting protocol works and have the base knowledge for exploring it in more detail.

E-Voting system defines a set of reference points between different E-Voting system entities and some of them use Diameter as the essential protocol to exchange Voters-, presence-, and Voter-related posts. As E-Voting system lasts to evolve, we trust there will be more e-voting Diameter requests to originate, as well as Diameter-related applications and operations.

REFERENCES