



**PROCEEDINGS OF THE
“SETMAPE”
RESEARCH AND
DEVELOPMENT
STREAM OF THE
AUSCERT 2008
CONFERENCE**

20 MAY 2008.

**Crowne Plaza Royal Pines Resort,
Gold Coast, Queensland.
Australia.**

SETMAPE

**Science, Engineering, Technology, Mathematics,
Policy and Education**

Edited by W. Caelli, AO

**Published by the
School of Information Technology
and Electrical Engineering
The University of Queensland
St. Lucia.
Queensland.
AUSTRALIA.**



**THE UNIVERSITY
OF QUEENSLAND
AUSTRALIA**

Program and Review Committee:

Chair:

Emeritus Professor William J (Bill) Caelli, AO
Director, International Information Security Consultants Pty Ltd, and
Senior Research Scientist, Information Security Institute – Queensland University of
Technology

Deputy Chair:

Professor Paul Bailes, Head, School of ITEE, The University of Queensland,
Queensland. Australia

Members:

Dr Cristina Cifuentes, Sun Labs Down Under, The University of Queensland
Dr Guido Governatori, School of Information Technology and Electrical Engineering,
The University of Queensland
Emeritus Professor Dennis Longley, Director, International Information Security
Consultants Pty Ltd., Queensland, Australia
Dr Vallipuram Muthukkumarasamy, School of Information and Communication
Technology, Griffith University Gold Coast Campus
Dr Juanma Gonzalez Nieto, Research Fellow – Information Security Institute and
Faculty of Information Technology, Queensland University of Technology
Dr Marius Portmann, School of Information Technology & Electrical Engineering
The University of Queensland, Queensland, Australia
Professor Corey D. Schou, University Professor of Informatics, Idaho State University,
Idaho. USA. and Director, National Information Assurance Training and
Education Center, Idaho. USA.
Mr Luke Wildman, System Safety and Quality Engineering Pty Ltd

ISBN 978-0-9805220-0-6

**Published by the
School of Information Technology and Electrical Engineering, The University of
Queensland. St. Lucia. Queensland. AUSTRALIA.
May 2008.**

TABLE OF CONTENTS

Keynote Paper: <i>Improving The International Computer Security Research Agenda Using Standards</i> C Schou Idaho State University Pocatello, Idaho. USA.	
<i>An easily validated security model for e-voting based on anonymous public key certificates.</i> S. Wilson	
<i>Making A CASE for PACE: Components of the Combined Authentication Scheme Encapsulation for a Privacy Augmented Collaborative Environment</i> G. Skinner	
<i>BANAID: A Sensor Network Test-bed for Wormhole Attacks</i> H Alzaid, S Abanmi , S Kanhere , Chun Tung Chou, F Alshuwair	
<i>Study of Timing Values in EAP Authenticated Wireless Hosts</i> J Silva, E Sithirasanen, V Muthukkumarasamy	
Appendix A: Call for Papers	

An easily validated security model for e-voting based on anonymous public key certificates

Stephen Wilson
Lockstep Technologies Pty Ltd
11 Minnesota Ave Five Dock NSW 2046 Australia
swilson@lockstep.com.au

Abstract

Most electronic voting solutions have so far been complex and correspondingly difficult for regulators to validate. We propose a simple and robust new security model for e-voting based on public key technology and ‘smart’ personal authentication devices (PADs) such as smartcards or SIMs. Highly tamper resistant digital signatures and public key certificates protect both the ballots and individual voters’ electoral enrolment. The solution can be deployed on a variety of modern smartcards, SIMs and so on, featuring built-in cryptographic processors.

Each electronic ballot cast using this solution is unique and anonymous. Ballots cannot be replayed, nor modified after lodgement. Repeat votes are readily detectable. The security model, based on mature PKI standards and commercial off-the-shelf components, is simple, transparent, and inexpensive to implement. Moreover, there is no reliance whatsoever on ‘security by obscurity’, rendering the solution easy to independently validate and certify.

Key words

D.4.6 [Operating Systems]: Security and protection – Authentication

K.4.4 [Computers and Society]: Electronic Commerce – Security

K.6.5 [Management of Computing and Information Systems]: Security and protection – Authentication

E.3 Data Encryption – Public key cryptosystems

J.1 [Administrative Data Processing] Government

Introduction and background

World wide experience of electronic voting to date has almost universally raised concerns about the quality and security of the underlying technologies and information systems. At best, e-voting systems have been criticised as lacking transparency. For instance, the Open Rights Group in its critical review of recent trials of e-voting in the United Kingdom commented that “E-voting is a ‘black box system’, where the mechanisms for recording and tabulating the vote are hidden from the voter (for more background on the United Kingdom trials, refer to the UK Electoral Commission website www.electoralcommission.org.uk). This makes public scrutiny impossible, and leaves statutory elections open to error and fraud” (Open Rights Group, 2007). At its worst, e-voting has been described as a “fiasco” for what some argue is a demonstrably disappointing standard of software engineering (Murdoch, 2007).

Following Britain’s local government internet voting pilots of May 2007, the United Kingdom Electoral Commission concluded that “the level of risk placed on the availability and integrity of the electoral process was unacceptable. There are clearly wider issues associated with the underlying security and transparency of these e-voting solutions ... which need to be addressed” (UK Electoral Commission, 2007). The

commission went on to strongly recommend a central process for testing and approving e-voting solutions.

One of the first places to attempt such a process was the state of California. After mixed experiences with commercial off-the-shelf e-voting solutions, the Secretary of State there initiated a “top-to-bottom” review of no fewer than four products, culminating in the high profile and unprecedented de-certification of all of them, in August 2007 (California Secretary of State, 2007).

Despite the challenges and the recent apparent setbacks, there remains a number of strong reasons to strive for secure electronic voting and, ultimately, trustworthy Internet-based e-voting. The important potential benefits include:

- improved voter turnout
- better availability and efficiency for absentee voting (providing defence force personnel with the capacity to vote when on duty overseas has been a special policy goal of Australia and the United States, amongst other nations, in recent years)
- reduced cost by avoiding the need for special voting equipment, which needs to be archived and/or maintained between elections.

While the focus of this paper is government elections, we should also remember that the medium of the Internet is ideal for a range of other polling and survey activities, such as opinion polling, deliberative polling, citizen initiated referenda, and company board elections. The demand for Internet based election and polling solutions is set to grow strongly.

Emerging standards for e-voting

While many critiques have been recently published (see e.g. Open Rights Group, 2007, Murdoch, 2007, UK Electoral Commission, 2007, and Rivest & Wack, 2006), perhaps the most elaborate and comprehensive attempt to standardise the requirements for e-voting has been that of the US National Institute of Standards and Technology’s *Voluntary Voting System Guidelines* (VVSG) (NIST, 2007). With respect to the security model of e-voting, there are two particularly significant requirements set down by NIST.

The first such requirement is for *Software Independence*, meaning that “an undetected error or fault in the voting system’s software is not capable of causing an undetectable change in election results”. NIST requires that all voting systems must be “software independent” in order to conform to the VVSG. A crucial feature of our anonymous certificate-based e-voting solution is that it is decoupled from the voter’s PC platform software, and is purely reliant on the compact secure firmware of a ‘smart’ Personal Authentication Device (PAD), which is far more amenable to independent verification. We outline with greater precision later in this paper what is meant by “smart” in this context. However, for clarity of expression, we will generally use the term “smartcard” to characterise a ‘smart’ PAD throughout the rest of this paper.

The reality is that e-voting software running on a commercial PC platform can probably not be proven to be secure; see *The nature of the software engineering challenge* below. This led NIST and other analysts to further recommend the feature known as *Voter Verifiability*, being the means for voters to be confident that their vote has been cast as intended. The NIST guidelines require that all voting systems include “a vote-capture device that uses independent voter-verifiable records (IVVR). IVVR can be audited

independently of the voting system software but do not necessarily have to be paper-based” (NIST, 2007).

The nature of the software engineering challenge

So why has developing robust e-voting systems been such a struggle? From first principles, we should expect difficulty when marrying mission and security critical applications to commercial operating system platforms. Complex fat client software is always hard to test, and fundamentally may be impossible to fully verify. Software quality professionals are generally familiar with the proposition tenet that “Finding all errors in a large system is generally held to be impossible ... or else highly demanding and extremely expensive”(Rivest & Wack, 2006).

It becomes especially prohibitive to manually inspect application code when its design makes it dependent on operating system code for its security functions; this is the case with almost all commercial software. Not only are many thousands, even millions of lines of code involved; it is not unusual for operating system vendors to keep details of their own software secret, in the interests of intellectual property protection. Such restrictions can be tolerated in most business applications, but with e-voting the social stakes are enormously greater.

Cryptographer and security expert Ron Rivest has written specifically on the e-voting challenge:

There is a fundamental problem we must face when trying to design remote electronic voting systems: the ‘secure platform problem.’ Cryptography is not the problem. ... The problem is interfacing the voter to the cryptography. Almost all proposed cryptographic voting protocols assume that a voter ... has a secure computing platform that will faithfully execute her portion of the protocol (Rivest, 2001).

We see the same fundamental ‘interface’ problem in all types of secure transaction system. Recent US Government standards for strong authentication over the Internet of high risk transactions recognise the inherent difficulty of protecting against attack when cryptographic keys are not protected in some form of hardware (NIST, 2006). The National Institute of Standards and Technology (NIST) has determined that to withstand man-in-the-middle attack (in which a spoof website might be put up in order to corrupt an online election) the only practical solutions entail hardware security devices and public key cryptography (Burr, 2005).

De-identification by anonymous certificate

In 2005 we published a detailed account as to how anonymous public key certificates can be used to bind individual smartcard holders to de-identified electronic health records or EHRs (Wilson, 2005). This technique can best be understood as creating a logical ‘triangle’ that binds together (1) an individual, (2) a smartcard that has been issued to them, and (3) a public key certificate issued against the smartcard that conveys some important attribute (in the case of an EHR, that individual’s unique health identifier). Importantly, the issuer of the smartcard and the issuer of the certificate need not be the same entity.

Note that the important characteristics of a ‘smart’ Personal Authentication Device include the following:

- automatic generation of public-private key pairs within the chip, with retention of the private key within the chip to mitigate against identity theft
- ability to perform all digital signing operations within the chip
- on-chip PIN verification (typically)
- other beneficial security enforcing functions such as mutual authentication to mitigate Man-in-the-Middle attack when accessing secure web sites such as polling sites.

The first objective of the EHR de-identification scheme was to ensure that when a record is created, all users of that record can be assured that it pertains to one particular individual, without revealing who that person was. It is critical to healthcare information management that electronic health identities are resistant to tampering and forgery, and that they cannot be stolen or replayed. We note that these same attributes are important in e-voting.

Let us now review how the de-identification solution works in its original context. Referring to Figure One, consider an individual patient named Smith to whom a Health Department has issued a Unique Health Identifier (UHI). If the UHI were to be carried around in an ordinary memory device and copied into transactions like regular data, then it would have no ‘pedigree’; that is, once the identifier is presented by the cardholder in a transaction, it behaves like any other numerical datum and is just as vulnerable to attack.

To better safeguard a UHI using a smartcard, the identifier can be ‘sealed’ into a public key certificate, as follows:

1. generate a fresh private-public key pair inside patient Smith’s smartcard
2. export a copy of the public key
3. create a certificate around the public key, including as an attribute the UHI
4. have the certificate signed by (or on behalf of) the Health Department.

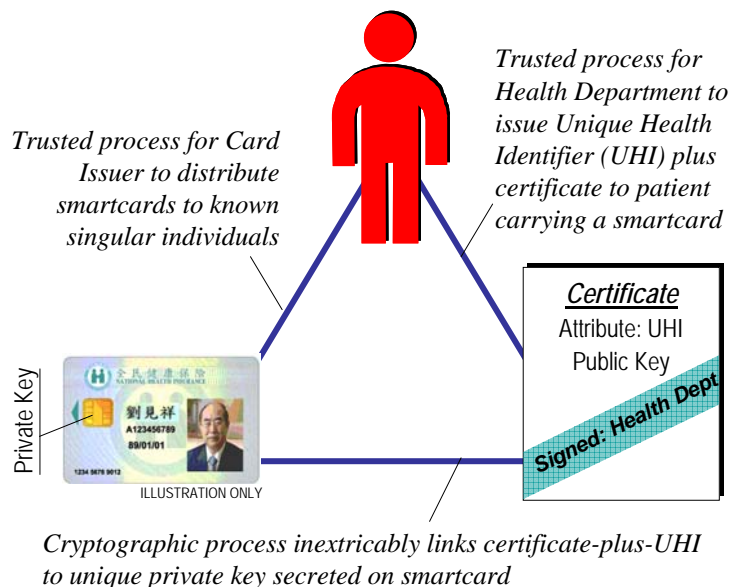


Figure 1: Logically ‘triangulating’ a smartcard, a patient and a unique health identifier

The result is a logical triangle that inextricably binds cardholder Smith to her UHI and to a specific smartcard. The certificate signed by the Health Department attests to Smith's ownership of both the UHI and a particular key pair unique to her smartcard. Private keys generated inside a smartcard are retained internally, and never divulged to outsiders. It is, for practical purposes, impossible to copy the private key to another card, so the logical triangular relationship is highly resistant to reproduction or counterfeiting.

Using anonymous certificates in e-voting

We now propose extending the concept of anonymous UHI certificates to secure e-voting, by arranging for a voter's de-identified electoral credentials to be notarised in a certificate associated with a smartcard, and using that smartcard to sign a ballot. As a result, individual ballots and the poll as a whole would be blinded with regard to the voter, but across the system we can be assured that each ballot is genuine and that no one has voted more than once.

Figure Two shows the major elements and processes of the e-voting solution, which are explained below.

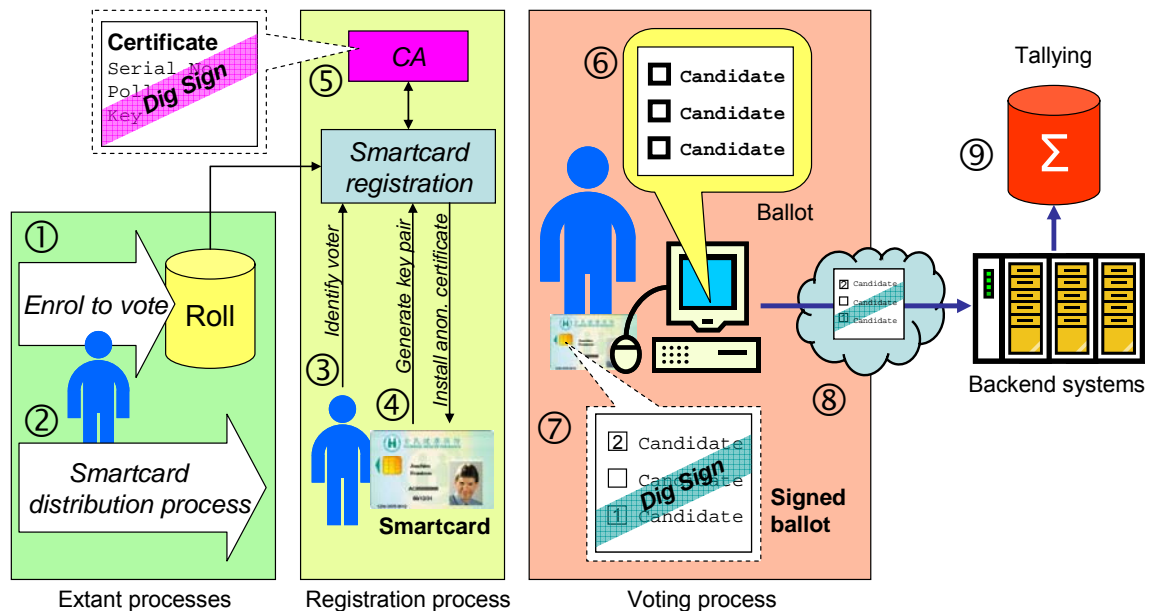


Figure 2: Components and workflows of the proposed e-voting solution

There are three major elements of the solution. The first element is a **smartcard** or functionally similar ‘smart’ PAD. used by the voter to secure their cast ballot. The smartcard carries a private key which is used to create a unique digital signature on the ballot. Note that the solution can be implemented using several alternatives to smartcards; as long as they have the requisite public key capability, the solution can use wireless PKI enabled cell phones, USB ‘crypto keys’, hardware security modules and so on.

The second element is an anonymous public key **certificate** issued to each registered voter, through a separate process that associates a smartcard with the voter’s electoral enrolment. The anonymous certificate contains:

- an indication of which election the certificate was issued for
- a serial number or other unique code that proves the uniqueness of the certificate, and
- a copy of the public key that matches the private key held in the smartcard.

The serial number is not ordinarily linked anywhere in the system to the identity of the voter. The certificate is signed by the relevant electoral authority, acting through a Certification Authority (CA), and contains nothing that identifies the voter. We will explain a little later that a ‘master file’ may be securely retained by the electoral authority if local voting election rules happen to require that ballots once cast be identifiable.

The third and final element of the solution is a **digitally signed ballot**, created using the smartcard and the public key certificate, interacting with standard PKI-enabled electronic forms software, with which ballots are composed (no doubt following a formal schema of some sort that enhances standardisation and data processing).

The major work flows and business processes in the proposed solution are set out below. Most of the processes are conventional in any election system. The act of casting a vote need not differ much from any other Internet polling system today, except for the inclusion of a smartcard in the work flow. Referring to the numbered steps in the diagram:

- **Enrol to vote:** Step ① shows the voter following whatever existing procedures and government policies are used to create and maintain a trusted electoral roll.
- **Distribute smartcards:** Step ② indicates an existing procedure for issuing suitable smartcards to individuals, including the business processes that deal with lost and stolen cards, card renewals and so on. Our proposal can be deployed into general purpose smartcards already distributed for banking, government services, identification and so on (see below), or alternatively, the e-voting solution could make use of dedicated cards.
- **Register a smartcard to carry voter entitlement:** Once individuals have smartcards, they will need to register their particular card to carry entitlements to vote in a given poll. This registration step can be carried out remotely in many cases – if there are remote access control arrangements in place that can be used to verify the card holder – or it can be carried out face-to-face at an electoral office or similar designated outlet. In detail, the technical steps involved are as follows:
 - At step ③ present the smartcard in a reader, either remotely or in person, and answer an identity challenge to prove ownership of the card as well as the good standing of their electoral enrolment (as established already in step ①)
 - At step ④ generate a public-private key pair in the smartcard chip (a seamless embedded process that goes un-noticed by the cardholder)

- At step ⑤ generate an anonymous voting certificate, and have it signed by or on behalf of the electoral authority (also seamless). Each certificate will contain a serial number or some other unique code allowing repeat votes to be detected when the signed ballots are later collated for counting.

When implementing the proposed security model in a real voting system, it is possible between steps ③ and ⑤ to retain a ‘master file’ that links certificate serial numbers to the identities of voters. In many electoral systems, an absolute guarantee of voter anonymity is desirable, and the natural implementation of our proposed solution would have the master file securely destroyed at this point. Yet in some jurisdictions – most notably the United Kingdom – it is a legal requirement that every voter’s ballot be available and identifiable after polling closes, in order to resolve disputes. Our solution allows for this possibility if the master file is archived rather than destroyed.

- **Cast votes:** Polls will open according to the particular election rules, and electronic ballots will be posted on a designated voting website for access by the public. Voters will log on to the site through a conventional security protocol such as Secure Sockets Layer (SSL) built into all web browsers and familiar to most users of Internet banking. The voter views the ballot at step ⑥ and indicates their choices through a suitable user interface.

When satisfied, they indicate their wish to submit the ballot, at which point the data with their selections is formatted and sent to the smartcard for signing. The ballot is signed using the unique private key matched to the anonymous voting certificate, at step ⑦. The signed ballot is then sent to the voting system backend at step ⑧. For convenience when validating signed ballots, the client side software will also send a copy of the voter’s anonymous certificate.

Note that any number of additional copies of the signed ballot may be saved at this point, for disaster recovery in the event of a loss of data later during counting, audit, and/or independent voter verification. For voter verification, a logical place to cache a copy of a signed ballot is the smartcard itself. The integrity feature of the digital signature means that all cached copies of a signed ballot are equivalent; none can be tampered with to create repeat votes or to alter a vote, because the signature will only validate against the unique anonymous certificate. If two *different* signed ballots are found with signatures that validate against the *one* certificate then we can be sure that the smartcard was used twice.

- **Count votes:** At step ⑨ after the poll closes, all cast votes are first checked for eligibility. In particular, all ballots’ digital signatures must correspond one-to-one to voting certificates issued for this particular election. Repeat usage of a single smartcard can be readily detected by looking for multiple instances of the same certificate. All validated signed ballots are then counted, and a poll result determined.

Smartcard compatibility

Our proposed e-voting solution is compatible with most PKI-enabled smartcards, as in widespread use for health services, government services, personal security, and national identity. Examples include the US military Common Access Card (CAC), the new US government Personal Identity Verification (PIV) card (NIST, 2005), the identity cards of Belgium, Estonia, Hong Kong, Malaysia, Sweden and Thailand, the government PKI services

card of Taiwan, and the new generation health cards of France (*Sesam Vitale*) and Germany (*Gesundheitskarte*).

Technically, any multi-programmable smartcard with a public key cryptography co-processor and on-chip key generation will be suitable for the proposed solution. A key length of 1024 bits or higher is nowadays standard, and an exposed application programming interfaces (API) is required for the voting server to update the smartcard and to trigger the signing of the ballot. Increasingly this sort of basket of security functions is being normalized by standards such as FIPS 201 as published by the US National Institute of Standards and Technology.

Discussion

Note that a host of accessibility and human factors engineering considerations lie outside the scope of this paper, where we have focused on the security model alone. Our proposed solution is compatible with any number of interface options as supported by today's standard PC and Internet platforms. Importantly, the ballot remains open to review and modification by the voter until they confirm their choices and instruct the smartcard to sign their ballot. That is, the proposal meets the new requirement of Voter Editable Ballot Device specified by the NIST VVSG (NSIT, 2007).

Before enumerating the specific security benefits of our proposal, let's review two special properties of the design.

Firstly it delivers a high fidelity form of voter verifiability of their ballots. At a minimum, an Independent Voter Verifiable Record (IVVR) may be produced as a tamper resistant soft copy of the digitally signed ballot. The copy may be cached in the voter's smartcard, where it would be available for review at any time. The smartcard's inherent PIN protection protects the privacy of the IVVR. Further, depending on implementation, there is the option of the voting system producing a printed copy of the ballot as cast, including a numeric rendition of the digital signature.

Secondly, in the context of the NIST requirements (NIST, 2007), our proposed solution is entirely independent of the software in the voter's host computer, typically a PC. The core security model is essentially implemented by firmware in the smartcard, wherein the voter's ballot is digitally signed using their dedicated and anonymously certified key pair. The only necessary cryptographic primitives are 'encrypt with internal private key' together with certificate lifecycle management commands such as 'generate key pair', 'fetch public key' and 'install public key certificate'. All of these are standard features of modern PKI-enabled smartcard firmware, and all are part of the target of evaluation for independent smartcard security accreditations.

The proposed new model brings a range of security benefits that have hitherto remained elusive in e-voting. With respect to our central claim of a simple and readily validated security model, our e-voting solution has the following benefits:

- The design makes use of a small set of mature cryptographic primitives that come built-in with most standard PKI-enabled smartcards today.
- The use of anonymous but otherwise entirely standard public key certificates and primitives requires no additional smartcard applets and involves zero perturbation to the design of most PKI-enabled cards; thus a smartcard's prior security accreditation is unaffected by the e-voting solution.
- The e-voting solution security is software independent with respect to the voter's host PC, to simplify end-to-end accreditation of the system.

- There is a strict, mathematically robust one-to-one mapping of signed ballots to anonymous public key certificates, making repeat voting essentially impossible.
- Each ballot cast is cryptographically unique, preventing replay attack; a vote cannot be cast without an authorised smartcard properly loaded with the anonymous registration certificate, and ballots once cast cannot be intercepted during transmission or storage and used to synthesise fake votes.
- Voter registration cannot be counterfeited, thanks to the digital signature of the electoral authority on the anonymous certificates.
- Copies of ballots can be cached as Independent Voter Verifiable Records, to provide redundancy and protection against system outages, denial of service attack and so on, without compromising the integrity of the ballot; all cached ballot copies can be reconciled later without possibility of double counting.
- The poll is readily auditable as each voter's public key certificate, while anonymous, is unique.

In addition to the special properties of the security model, our proposal brings several other general benefits for the conduct of trustworthy elections and other types of polling:

- Ballots are strongly blinded; voters remain anonymous and cannot be linked to their ballots (unless the registration master file is archived as may be required in certain jurisdictions).
- The smartcard represents a physical two factor authentication method (that is, it represents something the user knows plus something they possess) and so provides added protection against voter identity theft.
- Many smartcards can be configured with additional *mutual authentication* of the remote server, protecting the voter web site against spoofing.
- The solution is independent of detailed smartcard and card reader design (across a relatively wide class of PKI-capable cards) and can therefore be implemented as a value-add on numerous current platforms, such as driver licences, government services cards, identity cards and banking cards.
- The use of a thin client host platform means the solution is location independent and highly accessible, as is necessary for effective absentee Internet voting solutions.
- The design is inherently simple and therefore inexpensive to develop and deploy, from a software engineering perspective.

Conclusion

E-voting in general and Internet voting in particular represent significant technological challenges, not all of which are addressed by our proposal. In particular, service availability, resistance to denial of service attack, and resistance to hijacking of the host machine remain to be addressed.

Nevertheless, our proposal to secure electronic ballots using anonymous digital certificates represents a breakthrough in respect of a core set of important properties, including anonymity, resistance to replay attack and repeat voting, and resistance to counterfeiting. As smartcards, 'smart phones' and similar personal authentication technologies become more widespread, and as they become habitualised in peoples' regular Internet transactions, the proposal will become a practical and low cost option.

References

- BURR, W. (2005), Electronic Authentication in the U.S. Federal Government Asia PKI Forum Conference, Tokyo 2005 http://asia-pkiforum.org/feb_tokyo/NIST_Burr.pdf.
- CALIFORNIA SECRETARY OF STATE (2007) Top-to-bottom review of certified voting machines www.sos.ca.gov/elections/elections_vsr.htm.
- MURDOCH, S. J. (2007) The role of software engineering in electronic elections, University of Cambridge www.lightbluetouchpaper.org/2007/07/13/the-role-of-software-engineering-in-electronic-elections.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2005) Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201; available at <http://csrc.nist.gov/npivp>.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2006) Electronic Authentication Guideline, Special Publication SP800-63 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2007) Voluntary Voting System Guidelines: Recommendations to the Election Assistance Commission <http://vote.nist.gov/VVSG-0807/Final-TGDC-VVSG-08312007.pdf>.
- OPEN RIGHTS GROUP (2007) May 2007 Election Report Findings of the Open Rights Group Election Observation Mission in Scotland and England. www.openrightsgroup.org/wp-content/uploads/org_election_report.pdf.
- RIVEST R. L. (2001) Electronic Voting; www.vote.caltech.edu/Rivest-ElectronicVoting.pdf.
- RIVEST R. R. & WACK J. P. (2006) On the notion of “software independence” in voting systems <http://vote.nist.gov/SI-in-voting.pdf>.
- UK ELECTORAL COMMISSION AUGUST (2007) Electronic voting May 2007 electoral pilot schemes www.electoralcommission.org.uk/files/dms/e-votingresearchsummary_6782-6321_E_N_S_W_.pdf.
- WILSON, S. (2005) A novel application of PKI smartcards to 11anonymise Health Identifiers, AusCERT 2005 Security Conference Refereed Stream, Gold Coast, Australia, 2005 www.isi.qut.edu.au/events/conferences/auscert2005/proceedings/wilson05novel.pdf
- .

PAPER TITLE: Making A CASE for PACE: Components of the Combined Authentication Scheme Encapsulation for a Privacy Augmented Collaborative Environment

AUTHOR: Dr. Geoff Skinner

AFFILIATION: Faculty of Science and IT, The University of Newcastle.

CONTACT DETAILS:

Email: Geoff.Skinner@newcastle.edu.au

Phone: +61 (0) 2 4985 4512

Address: Room 3.13, ICT Building, The University of Newcastle, University Drive, Callaghan, Newcastle, NSW, 2308

Making A CASE for PACE: Components of the Combined Authentication Scheme Encapsulation for a Privacy Augmented Collaborative Environment

Abstract

The uptake and utility of digital collaboration's continues to grow as organizations are realizing the diverse range of benefits they provide to not only their organization as a whole but also to individual employees. However, like many information and communication technologies the implementation push often overshadows a proper evaluation of data security and information privacy risks that may be inherent with the technology. This paper details our ongoing research for addressing a number of authentication, access control, and personal entity identification issues encountered in digital collaborative architectures. We propose an authentication framework that uniquely combines both traditional and biometric methods of authentication with an additional novel audiovisual method of authentication. Further, the CASE (Combined Authentication Scheme Encapsulation) methodology provides an intuitive privacy protecting visual representation of a member entity's authentication methods, which is accessible by other member entities for help in assessing the risk of sharing 'sensitive' data with other collaboration entities and determining appropriate access controls.

1. Introduction

The underlying focus of many of the current Australian National Research priorities revolves around the idea of collaboration. Specific to the Information and Communication technology sector involves the promotion of digital collaborative architectures. In addition, related research priorities include improved data management and smarter information use which includes the protection of national information infrastructure. Our ongoing research and the topic of this paper

is centered on digital collaborations, in particular their use and support for fostering innovation. The evolution of innovative and creative ideas represent sensitive data that needs to be protected, more so when performed within shared environments like digital collaborations. As part of our continuing funded research in this field a number of technologies have been and are being developed to ensure sound data security and information privacy across collaborative digital architectures.

The research proposes to address and contribute to a number of important fields, particularly within the Australian Information and Communication Technology (ICT) sector. Currently Australia, like many other nations, faces a number of obstacles in not only finding effective means to encourage employees to partake in creative process to foster innovation, but also for them to share their ideas with others in a collaborative environment. To further complicate the situation a lack of suitable collaborative security and privacy controls as well as inadequate, confusing and inaccessible information on available controls contribute to employee's pessimism when contributing personal data and ideas to digital collaborations. To resolve some of these problems we have developed and continue to develop a number of solutions to improve data security and information privacy within digital collaborative architectures. Further, our solutions also make security and privacy information accessible to collaboration members presenting it in an easy to comprehend visual manner dynamically updated with each new personal or sensitive data access request.

Contained within this paper are details of two foundational components of our proposed Combined Authentication Scheme Encapsulation (CASE) methodology. As research is ongoing at the time of writing the full methodology and remaining parts

are not included. Rather, detailed discussion in section 4 is given to our novel Traditional, Audiovisual and Biometric (TAB) Authentication framework for integration with Privacy Augmented Collaborative Environments (PACE) [1]. Secondly, in section 5, we explain our unique Graphs Representing Authentication and Privacy Hierarchies (GRAPH) collaborative application. Background and related work are reviewed section 2, followed by an overview of a PACE in section 3. Section 6 provides a conclusion and section 7 the list of references.

2. Background and Related Work

The research issues we are addressing in relation to the areas of authentication and identification are driven by international recognition, academic and commercial, of problems with current security and privacy methods for data management [2]. While recent work [3, 4] has made some progress on improved data security and information privacy in collaborations, our research is unique in its plans to use a combination of authentication methods. To date no solutions have been proposed that uniquely combine traditional, audiovisual and biometric authentication methods into a single framework. The only similar proposals to our own have been work done on Multibiometric Systems [5] involving the use of multiple biometric devices, Webbiometrics [6] using soft biometric traits with a conventional login, and using a combination of an online signature with voice modalities [7].

The management of intellectual property within an organization [8] is another widely acknowledged problem, which becomes increasingly more difficult when organizations are engaged in collaborative activities [9]. As collaborations have shown to be highly effective means of increasing growth while saving costs for organizations [10], the members must remain conscience of the potential risks to the data they are sharing within the digital environment [11],

including new innovative and creative ideas. Most current technologies are unable to provide adequate protection of ‘sensitive’ data in digital collaborative environments [12, 13, 14].

Previous research involving the use of graph representations has focused primarily on access controls and other security specific components [15] and [16]. However, recent literature detailed similar approaches to our own but only the visual representation of configurations, activities, and implications of security mechanisms [17]. The most significant similarities are the use of a ‘pie’ graph which represents the ‘Impromptu Client Interface’. Importantly, industry leaders recognize the importance of visualization and collaboration describing them as being the ‘...strategic enablers of the upstream enterprise’ [18].

3. A Privacy Augmented Collaborative Environment (PACE)

Recent research by the author in the fields of Collaborative Architectures, Data Security and Information Privacy delivered a number of solutions for addressing privacy issues within digital collaborations [19, 20]. Inclusive to the research was the symbiotic combination of the individual components to produce a Privacy Augmented Collaborative Environment (PACE) [1] as represented in figure 1. The two foundational elements of a PACE include the PIVOTAL methodology (Privacy by Integration, Visualization, Optimization, Technology, Awareness, and Legislation) [19], and the TLC-PP framework (Technical, Legal, and Community Privacy Protection) [20]. Through the application of the PIVOTAL methodology and the TLC-PP framework collaboration owners can ensure sound data security and information privacy practices and protections that can be maintained within their digital collaborative environments. The remainder of this section explains the privacy protections of PACE and why a PACE should be used in combination with the proposed Combined

Authentication Scheme Encapsulation (CASE) methodology proposed in this paper.

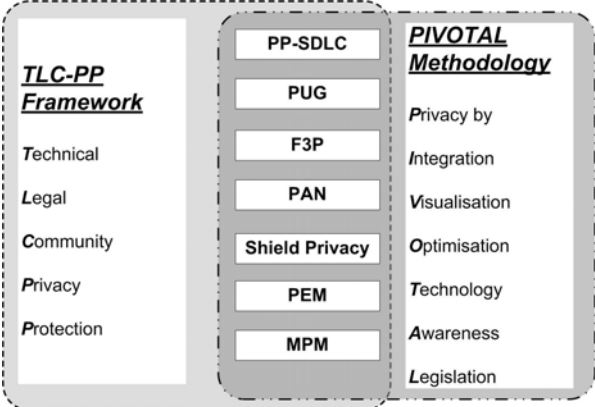


Figure 1: PACE Components

While the work of PACE was very successful in addressing information privacy problems in collaborative architectures it was unable to address a number of security issues related to member entity authentication, access control, and personal identification. That is, a member entity of PACE, the data provider (DP), was able to manage their personal or sensitive data. The DP was able to decide which other member entities had access to their data and how it could be used. The actual physical and system controls were still managed by the host systems, but the DP if given control could make informed decisions on who SHOULD have access and who SHOULD NOT. However, the data owners and therefore DP's were not able to verify with a high degree of certainty the 'personal' identity of the entity requesting data access, the data requestor (DR).

We highlighted this as a common problem in a digital collaboration and one we have termed authentication theft in our research context. Authentication theft refers to the specific problem encountered in PACE we address within our recent work detailed in this paper. Authentication theft unlike identity theft implies that only an entity's means of authentication are stolen. So if using traditional authentication methods an imposter would steal the username and password of a member entity

known to the data owner. The imposter could then request sensitive data from a member entity data owner under a false authenticated identity within the collaboration. That is, the imposter has managed to become a potentially valid and authenticated DR. From a digital collaboration systems perspective the provided username and password are correct so the imposter would be granted authentication into the collaboration. But the actual personal identity is false and therefore the data owner would be providing personal data to the imposter. Therefore the privacy protections provided with PACE need to be complimented with more stringent authentication methods that include the ability to verify what we term a 'personal' identity rather than just a 'system' identity in the context of our work.

The Privacy Protecting System Development Life Cycle (PP-SDLC) was the Integration element of the PIVOTAL methodology. It used a traditional form of the system development methodology that had information privacy considerations integrated into each of the life cycle phases. A similar approach should be used when integrating the 'personal' identity techniques into a digital collaborative architecture. The Visualization element is termed PUG for Privacy Using Graphs. PUG is an application available to member entities that can be used to dynamically map relationships between different entities. The details on the maps represent such things their degrees of separation from different entities in social structures, methods of security for both data at rest and in transit used by each member entity and also the level of access each mapped member entity has at time of graph generation. It is proposed that a similar application could be developed for CASE to represent the level or methods of 'personal' authentication each member entity has completed for their current session.

The Optimization element involved the creation of what is termed F3P for Fair Privacy Principles and Preferences. F3P

uses XML technology to represent a member entities privacy preferences pertaining to items of their personal or sensitive data. Again it is possible that in future work the preferences can be extended to support data representing the methods of authentication used by a member entity. The remaining three elements of Technology, Awareness, and Legislation were closely coupled with the TLC-PP framework.

To ensure comprehensive privacy protection within a digital collaboration three foundational factors are required as embodied with the TLC-PP framework. Firstly, the collaboration must continually integrate and update Privacy Enhancing Technologies within the collaboration. This principle is just as applicable to authentication technologies. Further, the current legal requirements must be enforced by the owners and administrators of digital collaborations. As legislation may develop to govern authentication standards for information systems collaborations must ensure the laws are enforced in their environments. Lastly, the member entities making up the collaboration's Community must be Aware of their privacy rights and also their privacy expectations. Therefore, as part of the collaboration's education efforts, details of authentication procedures can also be made available and publicized to the collaboration community. The next section details the proposed combined authentication scheme that should be integrated with the privacy protection measures used in PACE.

4. TAB Authentication for Collaborations

One of the key authentication contributions within the proposed CASE methodology is what we have termed the TAB framework. TAB represents a combined authentication scheme uniquely encapsulating Traditional, Audiovisual, and Biometric methods of authentication. The framework is composed of the respective three tiers of authentication that can be integrated into any digital collaborative

architecture and customized to each individual situation. Depending on the collaboration's data security and information privacy needs, in addition to the resources available, the TAB framework configuration can be modified to adapt and evolve with the collaboration.

The three levels or layers of the TAB framework and their methods of use are as follows:

- *Traditional*: in the context of our work the term Traditional refers to the more commonly available and frequently used methods of authentication that have been associated with weak levels of reliability. Traditional methods of authentication in our framework include the use of username/password combinations, Public Key Infrastructure (PKI) and Digital Signatures, Tokens, and Smartcards. In each form of Traditional authentication we classify them using the term 'System Authentication'. As mentioned in the previous section this implies that no personal individual identification of an entity is used in the authentication process.

For example, while a username/password combination may be unique to a single entity, a malicious entity may steal the username and password and use that to gain access to the digital collaboration and its resources. From the systems perspective it does not care who is using the username and password, it only matters that the correct username and password are provided. The same issue holds true for stolen smartcards, false tokens, and malicious use of stolen private-public key combinations with PKI. The motivation for our research is in part related to this inadequate method of authentication. In particular, we are concerned on its current common use for digital collaborative environment authentication. It is imperative in collaborative architectures that involve the sharing of personal or sensitive entity data, that the owner or custodian of the data in question can verify the 'personal' identity of the entity requesting the data.

As part of the CASE operational guidelines, we recommend that if a digital collaboration is only using Traditional means of authentication, then either member entities are made well aware of the potential risks to their data or the collaboration is only used for the sharing of non-sensitive or non-personal data. Preferably collaboration owners integrate the whole TAB framework into their architecture, so Traditional means of authentication can be used in combination with more ‘personally identifiable’ methods of authentication.

Our implemented prototype uses both username/password combinations in addition to Biometric enabled Smartcards. The smartcards used are Precise BioMatch Smart Card 64 which are Java based and for operation with Precise 200MC biometric readers. At time of writing plans are underway to integrate a PKI and generate public/private key combinations for use by all prototype member entities during further testing.

- *Audiovisual*: the second tier of the combined authentication framework involves the use of readily available audiovisual equipment. The uniqueness of the proposed approach is in the method of application of the tools for their use as real time authentication devices. Audiovisual authentication, in the context of our research, utilizes devices such as microphones or more preferably web cameras to stream live audiovisual footage of an entity, such as a data requestor, to another entity such as the data provider. The audio and streaming picture of an entity can be verified against registration media of the entity to provide real time authentication.

Verified registration media for the framework involves the submission of a recorded voice message of the registering entity in addition to submission of a high resolution image of them selves. The collaboration owners and administrators are tasked with ensuring the authenticity and verification of the initially provided media. An alternative we have investigated and implemented previously is the use of other

‘trusted’ member of the collaboration to verify and confirm the personal identity of a new member during registration. It would then be the responsibility of these entities to verify and ‘certify’ the authenticity of the provided media (voice print and digital photo) matching it with the known voice and personal appearance of the new registering entity.

The uniqueness of this approach is that through the use of a simple web camera a data provider can see, hear and interact with a data requestor at the time of the request. Our proposal is different from the formal biometric voice recognition authentication method, but provides many of the same benefits but in a more informal and real time setting. These benefits include audio and visual identification of an entity which provides a log or history of interaction. That is, once the personal identity of an entity has been seen and heard by another entity, that information is committed to memory. Therefore, after an initial audiovisual authenticated session it becomes increasingly harder for another entity to impersonate another.

Other advantages include a more personal level of interaction in addition to the relatively low cost of ownership for setting up the authentication infrastructure. As digital collaborations have benefits for all types of entities with equally diverse financial resources, audiovisual authentication offers a reliable, unique, and cost effective security solution. Our prototype environment uses entry level Logitech USB webcams and common messenger service applications to manage the streaming of audiovisual data. It is planned that we will develop our own collaborative environment plug-in application that integrates all three tiers of the combined TAB authentication framework and will manage audiovisual live streaming as part of its functionality.

- *Biometric*: the third or ‘top’ tier in the TAB framework hierarchy is Biometric authentication. There is considerable literature, as discussed in Section 2,

supporting biometric devices as being the most reliable form of authentication and identification currently available. However, in the three classifications used for the TAB framework, it also represents the most expensive and resource intensive to purchase, install, and manage. As such we have placed biometric authentication in the third tier and recommend its use for collaborations that manage personal or sensitive data on a regular basis. To do envisage and encourage with our own framework that as prices for biometric devices continues to decrease then biometric authentication would be mandatory in all forms of digital collaborative environments.

The TAB framework is designed for maximum flexibility and adaptability. Therefore, the TAB conceptual framework does not require a specific biometric device; rather any biometric device can be used for authentication when implementing TAB. With much debate in the literature on what is a more reliable form of biometric device the TAB framework accommodates a broad spectrum of biometric preferences. The only requirement is that an ‘enrollment and test’ is carried out for each member entity. That is, when a new entity registers to become a member of the digital collaboration they must have their biometric information (the template) securely collected and stored within the collaboration. Then each time the member entity authenticates with the collaboration their biometric scan is tested for a match with the stored template. In this manner the TAB framework uses Biometric authentication for both verification and identification. Our working prototype currently uses the Precise 200 MC fingerprint reader from Precise Biometrics [21] at each of the collaborations test nodes. Theses devices have a combined fingerprint and smart card reader providing all required biometric matching and smart card functionality that is securely processed within the device or the smart card.

The TAB framework is intentionally flexible in nature and design so it may be integrated with many forms of digital

collaborative architectures. Rather than each tier specifying a specific method of authentication, there is sufficient scope to adjust to individual preferences at each distributed site or node of the collaboration. This conceptual approach to the design of the framework allows the implementation to continually evolve with updates in technologies and authentication processes. The next section explains how the TAB framework is visually represented in a digital collaboration so its members can determine how each of the other member entities is currently authenticated with the collaboration. The TAB framework in addition to the visual representation of the authentication methods are two key components of the CASE methodology.

5. Visualizing the CASE 4 PACE

The main contributions of this paper are the proposals and defining of two key components of the CASE methodology. That is, rather than trying to just outline the complete CASE methodology in a single paper we have focused on two of CASES unique elements and primary contributions. The first being the TAB framework proposed in the previous section. The second, and subject of this section, is our novel GRAPH (Graphs Representing Authentication and Privacy Hierarchies) collaborative application for assistance in managing data security and information privacy in digital collaborative architectures. The remainder of this section is used to explain the details of the GRAPH application including its integration into a digital architecture and its role within the CASE methodology. As GRAPH is still under development no operational screen shots are available, however figures 3 and 4 respectively show the conceptual representations of what an ‘Entity Node’ and what we have termed ‘DEAN’ (Dynamic Entity Association Network) graph will convey when produced by the completed GRAPH application.

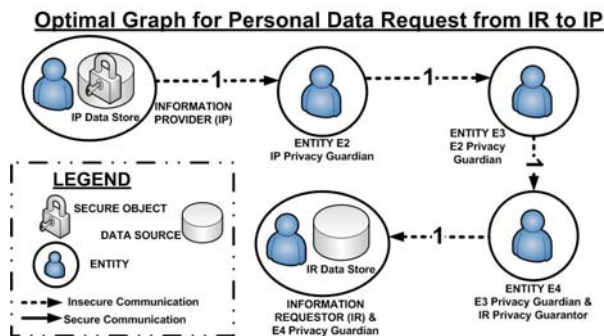


Figure 2: Previous PUG presentation of data security and information privacy relationships

The GRAPH application represents on evolution of a previous information privacy management software utility we have developed entitled Privacy Using Graphs (PUG) [1]. As PUG already provided a visual representation of information privacy relationships between entities within a digital collaboration, as shown in figure 2, it therefore was an ideal foundation for adding security representations such as an entity's method or methods of authentication. The next step was to devise a minimalist method of visually representing the three authentication classifications or tiers defined by the TAB framework. It was envisaged that the application would be used in global collaborations so a universally recognized representation was required which was also capable of conveying a number of different states within each tier's representation.

It was decided that a set of three traffic light signals should be used, one for each tier of the TAB framework. The color of each respective authentication traffic light (green, yellow, or red) corresponds to the completeness of meeting the authentication conditions within each tier for the current session. That is, the different colored lights have analogies similar to real world traffic lights.

- **RED**: indicates that no authentication conditions are fulfilled under this tier. For example, in figure 2, the audiovisual authentication traffic light (A) is red and therefore the entity in question is not currently using audiovisual authentication, neither audio nor visual.

- **YELLOW**: indicates that only partially authentication conditions are fulfilled under this tier. For example, in figure 2 the traditional authentication traffic light (T) is yellow so the entity in question may have provided only a username and password but not completed a smart card or PKI based authentication process during this session.

- **GREEN**: indicates that all authentication conditions are fulfilled under this tier. For example, in figure 3, the biometric authentication traffic light (B) is green indicating that in our prototype the entity in question has used either finger print or iris scanning authentication processes during this session.

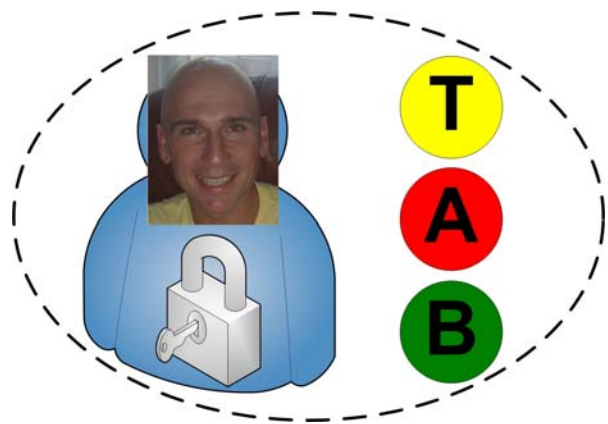


Figure 3: Entity node representation using the GRAPH collaborative application for security and privacy.

An additional personal identification feature we have included with GRAPH involves displaying on their graph node. Member entities at time of registration and enrolment have the option of providing a high resolution photo of them selves which is then subjected to verification and certification for use in the collaboration. Each session when an entity authenticates with the collaboration they will have the option of making their personal identification photo available for public access on their node within the GRAPH application, in addition to it being accessible as part of their collaboration profile. The individual elements of a collaboration profile, such as the personal photo, can be configured for accessibility by other

- [3] C. Yang, F.O. Lin, and H. Lin, "Policy-based Privacy and Security Management for Collaborative E-education Systems," in Proceedings of the 5th IASTED International Multi-Conference of Computers and Advanced Technology in Education (CATE 2002), Cancun, Mexico, May 2002.
- [4] J.B. Spira, "Privacy in the Collaborative Business Environment," KM World, November 2004.
- [5] A.K. Jain and A. Ross, "Multibiometric Systems," Communications of the ACM, vol. 47, no. 1, January 2004.
- [6] H. Gamboa, A.L.N. Fred, and A.K. Jain, "Webbiometrics: User Verification Via Web Interaction," in Proceedings of Biometrics Symposium, 2007, pp: 1-6.
- [7] S. Krawaczyk and A.K. Jain, "Securing Electronic Medical Records using Biometric Authentication," Lecture Notes in Computer Science, vol. 3546, 2005, pp: 1110-1119.
- [8] L. Johnson, "Managing Intellectual Property for Distance Learning," Educause Quartley, vol. 29, no. 2, 2006.
- [9] M. Angelaccio, A. D'Ambrogio, "A Model Transformation Framework to Boost Productivity and Creativity in Collaborative Working Environments", Proceedings of the 3rd International Conference on Collaborative Computing: Networking, Applications and Worksharing, New York, USA, November 12-15, 2007.
- [10] L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke, "A Community Authorization Service for Group Collaboration," in Proceedings 3rd International Workshop on Policies for Distributed Systems and Networks, 2002, pp: 50-59.
- [11] D. Argarwal, M. Thompson, M. Perry, and M. Lorch, "A New Security Model for Collaborative Environments," Lawrence Berkeley National Laboratory, University of California, CA, USA, Paper LBNL-52894, 2003.
- [12] E.F. Churchill, D.N. Snowdon, and A.J. Munro, Collaborative Virtual Environments: Digital Places and Spaces for Interaction, Springer-Verlang, 2001.
- [13] I. Traore and S. Khan, "A Protection Scheme for Collaborative Environments," in Proceedings of the 2003 ACM symposium on Applied Computing, 2003, pp: 331 - 337.
- [14] P.A. Dargon, "The Ideal Collaborative Environment," The Journal of Defence Software Engineering, vol. 14, no. 4, April 2001, pp. 11-15.
- [15] R. Sandhu, "A Perspective on Graphs and Access Control Models," Lecture Notes In Computer Science (LNCS), vol. 3256, November 2004, pp. 2-12.
- [16] M. Kock et al, "A Graph Based Formalism for RBAC," in ACM Transactions on Information and System Security (TISSEC), vol. 5, iss. 3, 2002, pp. 332-365.
- [17] R. de Paula et al, "Two Experiences Designing for Effective Security," in Proceedings of the 2005 symposium on Usable privacy and security, vol. 93, 2005, pp. 25-34.
- [18] E.J. Dodd, "Visualization and Collaboration for the On-Demand Upstream Petroleum Enterprise," IBM Industry White Paper, May 2004, <http://www-03.ibm.com/industries/ca/en/chemicalspetroleum/petroweb/wpapers.html>.
- [19] G. Skinner, "The TLC-PP Framework for delivering a Privacy Augmented Collaborative Environment (PACE)", in proceedings of The 3rd International Conference on Collaborative Computing, Networking, Applications and Worksharing, New York, USA, November 12-15, 2007.
- [20] G. Skinner, "Setting the PACE: a Privacy Augmented Collaborative Environment using the TLC-PP Framework", in proceedings of First International Workshop on Sustaining Privacy in Autonomous Collaborative Environments (SPACE 2007), July 30th – August 2nd, 2007, Moncton, New Brunswick, Canada.
- [21] Precise Biometrics, Precise 200MC, <http://www.precisebiometrics.com/?id=229&cid=397>.

BANAID: A Sensor Network Test-bed for Wormhole Attacks

Hani Alzaid

halzaid@isi.qut.edu.au

Information Security Institute
Queensland University of Technology,
P.O Box 2434, Brisbane, Queensland 4001,

Suahail Abanmi, Salil Kanhere, Chun Tung Chou

{abanmis, salilk, ctchou@cse.unsw.edu.au}

School of Computer Science and Engineering
University of New South Wales
Sydney, NSW 2052
Australia

Faisal Alshuwair

shuwaier@kacst.edu.sa

Computer and Electronic Research Institute
King Abdul-Aziz City for Science and Technology
P.O Box 361050, Riyadh 11313, Saudi Arabia

BANAID: A Sensor Network Test-bed for Wormhole Attacks

Abstract

The development of wireless sensor devices in terms of low power and inexpensive data-relaying has been partially achieved because of the rapid progress in integrated circuits and radio transceiver designs and device technology. Due to these achievements, the wireless sensor devices are able to gather information, process them if required, and send them to the next sensor device. In some applications, these wireless sensor devices must be secured, especially when the captured information is valuable, sensitive or for military usage. Wormhole attacks are a significant type of security attacks which can damage the wireless sensor networks if they go undetected. Unfortunately, these attacks are still possible, even if the communication is secured. The wormhole attack records packets at one point of the network, passes them into another node and this last node injects the packet into the wireless sensor network again. This type of attacks can not be avoided by using cryptographic techniques because attackers neither generate new nor alter existing packets. They only forward legitimate packets from part of the network to another part. This attack can cause damage to the route discovery mechanism used in many routing schemes. In this paper we build an actual test bed to simulate the wormhole attack on a wireless sensor network and then implement one of the current solutions against this attack. This test bed consists of a combination of Mica2 motes and Stargate sensor devices.

1. Introduction

The capability of combining sensing, processing, and communicating wirelessly have been enabled by the advances in microelectronics fabrication [2]. A Wireless Sensor Network (WSN) is composed of a group of tiny sensor devices, which can be networked together and deployed in a wide spectrum of applications in various military and civil domains. The main objectives of deploying the Wireless Sensor Network (WSNs) are remote monitoring and gathering information [2]. Most of WSN's applications run in non-trusted environments and require secure communications such as emergency response operations, military or police networks, and safety-

critical business operations. For example, in emergency response operations such as after a natural disaster like flood, tornado, or earthquake, a wireless sensor network could be used for real time feedback. So, emergency rescue will rely on that particular type of networks [3].

Unfortunately, this type of network is vulnerable to several attacks. One major type of these attacks is known as a Wormhole attack where an attacker records a packet at one location in the network, tunnels the packet to another location, and replays it at other part of the network [3]. The wormhole attack places the attacker in a very powerful position, allowing him to gain unauthorized access, disrupt routing, or perform a Denial-of-Service (DoS) attack [3]. Current solutions for Wormhole attack such as [4, 9,10] are evaluated by running the proposed techniques in different simulations. There is no real deployment for any of these solutions. To the best of our knowledge, this is the first work that built an actual test bed to show the visibility of the Wormhole attack in WSN. The test bed consists of few numbers of Mica2 [1] and two Stargate [2] sensor devices. Moreover, one of the proposed solutions, which is Packet Leashes [4], will be implemented.

The rest of the paper is organized as follows. In Section 2, an introduction about different components used in building up the test bed will be given. Section 3 describes the designing and the implementation of the test bed. Section 4 concludes the paper.

2. Test Bed Components

It is important to have some background about the wireless sensor devices used in this paper to build up the test bed. The test bed consists of several Mica2 motes and two Stargate sensor devices. In the following subsections, brief information about these two types of wireless devices is given.

2.1 MICA2

There are different models of Motes that have been produced by Crossbow¹. Each of these models has different features. These models are MICAz, MICA2, MICA2DOT, and MICA. All models except MICA2 are beyond the scope of this project. MICA2 Motes have been used in this project to build the test bed. Therefore, the features, hardware layouts, and software environment of MICA2 Motes are described in the following subsections.

2.1.1 MICA2 Features

The MICA2 Motes come in three types according to their RF frequency band: the MPR400 (915 MHz), MPR410 (433 MHz), and MPR420 (315 MHz). The Motes use the Chipcon CC1000, FSK modulated radio. All types utilize a powerful Atmega128L micro-controller and a frequency tunable radio with extended range. The MPR4x0 and MPR5x0 radios are compatible and can communicate with each other. (The x = 0, 1, or 2 depending on the type / frequency band) [1]. Figure 1.1 shows a sample of MICA2 Mote.

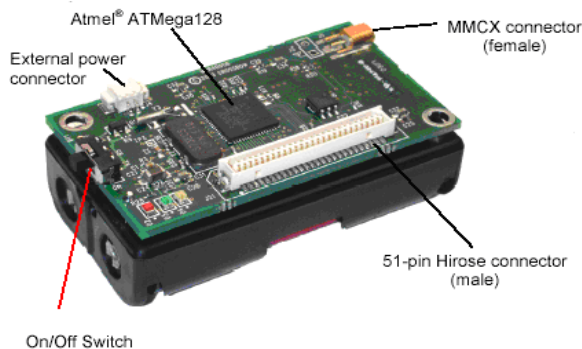


Figure 1: MICA2 Motes without an antenna [1].

The current version of Mica2 uses a 16 bit, 8MHz Texas Instruments, 1024 KB external flash, and is powered by two AA batteries.

2.1.2 Hardware Layout

The MICA2 Mote can be reprogrammed using an external board called MIB510 Serial Interface Board. This board is a multi-purpose interface board used with MICA, MICA2, MICAz, and MICA2DOT Motes family. It supplies power to the devices through an external power adapter option, and provides an interface for a RS-232 Mote serial port and reprogramming port [4].

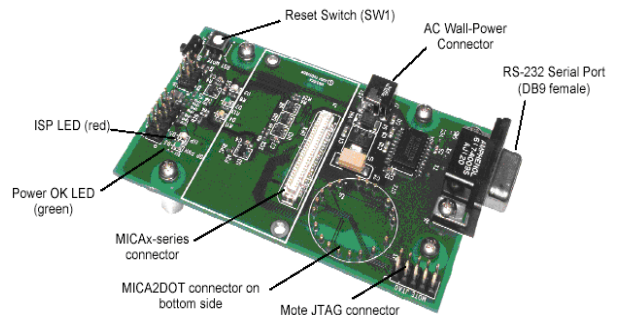


Figure 2: MIB510 Serial Interface Board [1].

The MIB510 serial interface board, as shown in Figure 2, is used to program the MICA2 Mote. This board has the PC connection capability using the RS-232 serial port. Programming the Motes requires a special operating system called TinyOS, which should be installed in the PC.

2.1.3 Software Environment

MICA2 Motes uses a special operating system, which is used for wireless sensor nodes, called TinyOS [7]. This operating system is an open-source event-driven operating system designed for wireless embedded sensor networks. It features a component-based architecture which enables rapid innovation and implementation while minimizing code size as required by the severe memory constraints inherent in sensor networks. TinyOS's component library includes network protocols, distributed services, sensor drivers, and data acquisition tools – all of which can be used as-is or can be further refined for a custom application. TinyOS's event-driven execution model enables fine-grained power management, yet allows the scheduling flexibility made necessary by the unpredictable nature of wireless communication and physical world interfaces [1]. TinyOS have been implemented in a language called nesC. This language is an extension to C which has been designed to

¹ <http://www.xbow.com/Home/HomePage.aspx>

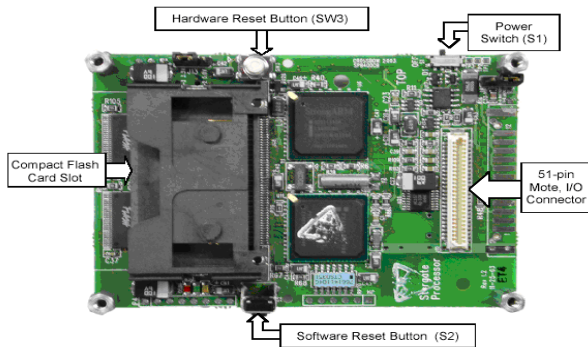


Figure 3: Processor Board (Top View)[2].

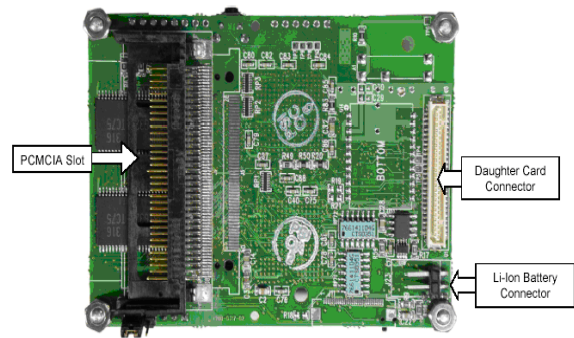


Figure 4: Processor Board (Bottom View) [2].

embody the structuring concepts and execution model of TinyOS. Programs written in nesC language are built out of components, which are wired to form entire programs. Each component has interfaces which can provide its functionality to other users.

2.2 Stargate

Stargate is a powerful single board computer with enhanced communications and sensor signal processing capabilities. This product was designed within Intel's Ubiquitous Computing Research Program, and licensed to Crossbow for production. In addition to traditional single board computer applications, the Stargate directly supports applications around Intel's Open-Source Robotics initiative as well as TinyOS based Wireless Sensor Networks.

2.2.1 Stargate Features

Stargate uses Intel's latest generation 400 MHz XScale processor (PXA255) and SA1111 StrongARM companion chip for I/O access. It has a reset button, real time clock, lithium ion battery option and 51-pin daughter card interface [2]. The Stargate sensor device used in this test bed has various features which can also be used in different applications. The main feature that has been used extensively in the test bed is the Compact Flash slot. Stargate has the capability to have a WiFi Compact Flash card. Another expansion in Stargate is MICA2 Mote connector, which allows the Stargate to communicate with other MICA2 Motes through the radio channel. Stargate consists of two hardware pieces: the processor board and the daughter card. These pieces will be explained in details in the following subsection

2.2.2 Hardware Layout

As mentioned in the previously, Stargate consists of two hardware pieces: a processor board and a daughter board. Each of these pieces will be described in this subsection. The processing board as appeared in Figure 3 and Figure 4 shows all the main buttons and slots. Figure 3 shows the top view of the processing board. It is clear from this view that

Stargate has two slots. These slots can be used to communicate with other devices. The first slot is used to allow Stargate to communicate with other MICA2 Mote by connecting a MICA2 Mote over the Stargate. The second slot is used to connect WiFi Compact Flash card to the Stargate, which allow it to communicate through the standard 802.11a or 802.11b wireless protocols.

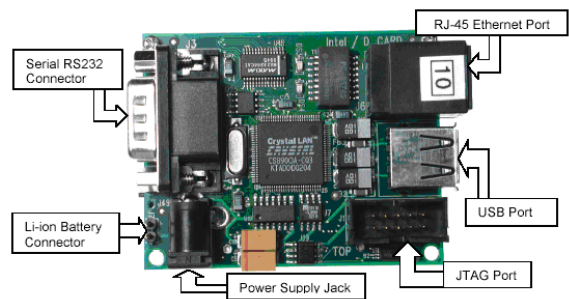


Figure 5: Daughter Card (Top View) [2].

The processor board gets its power from the daughter card. The daughter card has a power supply jack as it appears in Figure 5 and Figure 6. Also, the daughter card allows the user to communicate with Stargate using different types of interfaces. There are three different ways to communicate with Stargate. The first one is using Serial RS232 Connector.

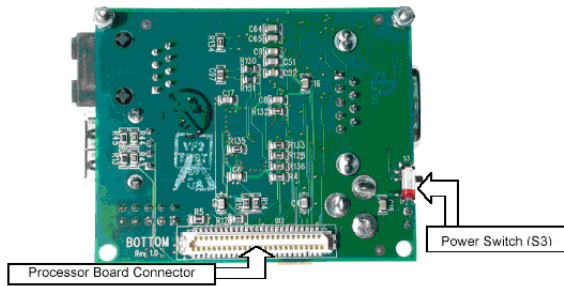


Figure 6: Daughter Card (Bottom View) [2].

The second is using RJ-45 Ethernet Port. And the third one is using USB Port. All these interfaces give the ability to control or upload programs to the Stargate. All switch buttons in the Stargate processor board and daughter card have to be switched on before using Stargate. There are two switch buttons S1 and S2 in the processor board. The third switch button S3 is located in the daughter card.

2.2.3 Software Environment

As mentioned before, the Stargate is using an embedded Linux operating system kernel. It is installed on the processing board of the Stargate. There is also additional software shipped with the Stargate development platform, which could be used to enable program development. The Stargate's platform provides the capability of installing programs written in C language. The developer can control various functions in Stargate by using C language programs after compiling and installing them.

3. Building the Test Bed

In this section the design, implementation, explanation of the wormhole attack, and the implementation of its solution will be described.

3.1 Design of the Test bed

The proposed test bed is developed with the following underlying assumptions:

- The chosen network topology is assumed to be fixed.
- Each node is assumed to know its neighbors.

Figure 7 shows that the test bed is composed of seven Mica2 sensor nodes and two Stargate devices. In this network design, the original source is Mote 1 and the original destination is Mote 4. The global clock is a normal sensor (Mote) which keeps sending a clock packet to synchronize all other motes.

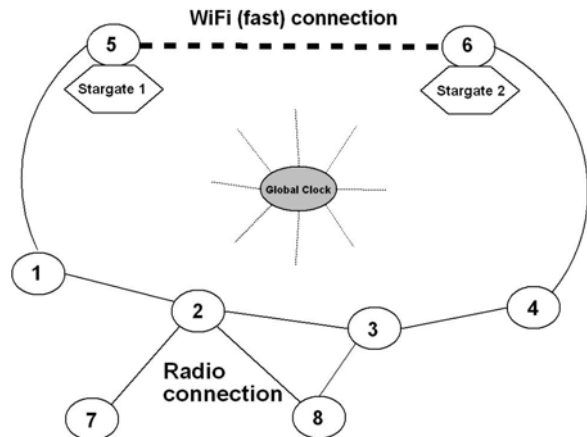


Figure 7: The proposed design of the test bed.

Each Mote in each Stargate will only forward any received message from radio connection to WiFi connection and vice versa without changing these messages. The routing algorithm that has been used in this test bed is the Ad hoc On Demand Distance Vector (AODV). This routing algorithm will be explained in the next section.

Moreover, the wormhole attack happens during the phase of building the routes between nodes in AODV. The attack will affect the routing table entries in the original source and destination motes. Therefore, the actual path that a message should pass from the original source to the original destination will be imprecise. The impact of the wormhole attack on the network will appear clearly in both the original source and the original destination motes. The original source mote will deal with the original destination mote as its direct neighbor and vice versa, which is not right because they are separated by two intermediate motes.

3.2 The AODV Algorithm

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources.

AODV builds routes using route request and reply query messages. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet

update their information for the source node and set up backwards pointers to the source node in the route tables. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination and the sequence number in RREQ packet is not present in the node. If this is the case, it sends a RREP back to the source. Otherwise, it forwards the RREQ. Nodes keep track of the RREQ's packets by storing their sequence numbers. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

As the RREP propagates back to the source nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. The routing table for each node will be updated according to the hop count field in RREQ or RREP packets. The received packet with the smallest hop count will be chosen as the best route path.

However, in this paper, not all of AODV routing algorithm features have been implemented, features that meet the aim of this project are just implemented for the sake of simplicity. For example, features like sending and receiving RREQ/RREP packets, and building the routing tables for each node have been implemented whereas features like maintaining the route paths and sending hello messages have not been implemented.

3.3 The implementation of the test bed

According to the proposed design of the test bed, there are seven MICA2 Motes and two Stargate sensor devices. Two motes have been combined with the two Stargate sensor devices which are mote 5 and mote 6.

To implement the test bed, three types of programs have been written and installed in the motes and the stargate sensor devices. The first program has been installed in motes 1, 2, 3, and 4, which is a simple customized AODV algorithm. The second program has been installed in motes 5 and 6, which forwards any received packet from the radio antenna to the serial port that connects the mote with the Stargate and vice versa, without changing this packet. The third program has been installed in both Stargate 1 and 2. When a packet is received by the Stargate from its serial port, which is connected to the corresponding mote, the program forwards it to the other Stargate through its WiFi connection and vice versa. The other Stargate will receive this packet from its WiFi

connection and forward it to its serial port, which is also connected to the corresponding mote. Then this packet will be broadcasted via the radio antenna of the mote.

3.3.1 The AODV Program

Before describing the functionalities that are done by this program, a brief explanation about the important variables is given as follows:

OS	OD	C	N	HC	MID	MT	S/M	TS
----	----	---	---	----	-----	----	-----	----

Table 1: Packet Format.

Table 1 illustrates the packet format used in building this test bed where

- **OS** represents original sender address.
- **OD** represents original destination address.
- **C** represents the current sensor address.
- **N** represents the next sensor's address.
- **HC** represents the hop counter.
- **MID** represents the messages ID.
- **MT** represents the message type.
- **S/M** explains whether the message comes from a Stargate or a Mica2 sensor.
- **TS** represent time stamp.

Dest. Address	Next Hop	Hop Count
...		

Table 2: Routing Table Format.

Next, Table 2 describes the routing table format. It is a $k \times 3$ array where k is a predefined value that represents the maximum number of entries that the routing table can hold. The table consists of three fields: the *destination address* field which stores the final destination for the current received packet, the *next hop* field which holds the address for next hop, and the *hop count* field which represents the number of hops left before reaching the final destination.

Figure 8 illustrates the pseudo code² that has been used in this paper to implement AODV. It describes the AODV's functionalities that have been implemented in order to build this test bed.

² The whole program can be obtained by contacting the first author.

Algorithm 1: AODV Program

```
1:  intilization phase;
2:  send PKT;
3:  run server thread with IP:10.1.1.2;
4:  synchronize internal clock with the global clock;
5:  if PKT_MSG_Type == 0 then // RREQ mode
6:    if PKT_MSG_ID is not in RREQ list then
7:      add entry into Routing Table;
8:      add PKT_MSG_ID into RREQ list;
9:      if PKT_Orign_Destin == Current_Mote_Address then
10:       prepare RREP PKT and send it;
11:     else
12:       forward PKT;
13:     end if
14:   else
15:     check RT for PKT_Orign_Source and get the Hop_Count;
16:     if Hop_Count > PKT_Hop_Count then
17:       update the entry in Routing Table;
18:       send PKT;
19:     end if
20:   end if
21: else if PKT_MSG_Type == 1 then // RREP mode
22:   if PKT_MSG_ID is not in RREP list then
23:     add entry into Routing Table;
24:     add PKT_MSG_ID into RREP list;
25:     if PKT_Orign_Destin == Current_Mote_Address then
26:       prepare RREP PKT and send it;
27:       send routing information for this mote;
28:     else
29:       forward PKT;
30:     end if
31:   else
32:     check RT for PKT_Orign_Source and get the Hop_Count;
33:     if Hop_Count > PKT_Hop_Count then
34:       update the entry in Routing Table;
35:       send PKT;
36:     end if
37:   end if
38: else if PKT_MSG_Type == 2 then
39:   if PKT_Orign_Destin == Current_Mote_Address then
40:     packet reaches its destination;
41:   else
42:     check RT for PKT_Orign_Source and get Next_Hop;
43:     send PKT for the next hop;
44:   end if
45: end if
46: end if
```

Figure 8: Pseudo Code of AODV.

It does the most important part of this project since it implements the AODV routing algorithm, synchronizes with global clock, and implements the a solution to the wormhole attack. This program has been written in combination of nesC and C languages and will be upload into Mote 1,2,3, and 4.

Algorithm 2: TOSBase Program

```
1:  intilization phase;
2:  if Radio receive msg then
3:    call UARTSendTask to send msg;
4:  end if
5:  if UART receive msg then
6:    call RadioSendTask to send msg;
7:  end if
```

Figure 9: Pseudo Code of TOSBase.

3.3.2 TOSBase Program

This program was written and delivered with the TinyOS tool kit as one of many readymade applications.

Algorithm 3: Stargate Program

```
A: Stargate One's Program
1:  intilization phase;
2:  open serial port;
3:  run server thread with IP:10.1.1.2;
4:  // the previous command runs forever to receive any
5:  // msg from Stargate2 with IP:10.1.1.3 and forward it
6:  // to the serial port to be sent by Mica2 sensor via radio
7:  for (1) do
8:    if Stargate receive a msg from the serial then
9:      if msg comes from mote 1 and it is RREQ then
10:       call client to forward the msg through WiFi to Stargate2;
11:     end if
12:   end if
13: end for

B: Stargate Two's Program
15: intilization phase;
16: open serial port;
17: run server thread with IP:10.1.1.3;
18: // it runs forever to receive any msg from Stargate1 with
19: // IP:10.1.1.2 and forward it
20: // to the serial port to be sent by Mica2 sensor via radio
21: for (1) do
22:   if Stargate receive a msg from the serial then
23:     if msg comes from mote 4 and it is RREP then
24:       call client to forward the msg through WiFi to Stargate1;
25:     end if
26:   end if
27: end for
```

Figure 10: Pseudo Code of Stargate's Program

The name of this application is TOSBase, which can be found under the application directory in TinyOS file. Figure 9 lists the functionality of this program. It simply forwards any received packet from the radio antenna of the Mica2 sensor to the serial port (51-pin Hirose Connector), which is shown in Figure 1, without changing the content of the packet. The Mica2 sensor is connected to the Stargate through this serial port. This program is written in nesC language and will upload into Mote 5, and 6 (see Figure 7).

3.3.3 Stargate Program

The program consists of two threads or processes³. The first process is the main program, which keeps listening to the serial port connected to the mote and sends any received packet to the client socket. The client socket will initiate a WiFi connection with the server socket in the other Stargate. The second thread or process runs as a server that keeps listening to any client connection via WiFi. It receives the packet and forwards it to the serial port connected to the mote, which will broadcast the packet via its radio antenna. As explained in Figure 10, the program in Stargate 1 will only forward messages from radio that comes from the original source which is mote 1. The other Stargate 2 will only forward messages from radio that comes from the original destination mote 4. The two versions of these

³ The whole program can be obtained by contacting the first author.

programs are the same except in checking the type of the message before start forwarding it.

3.4 Demonstration of the test bed

This subsection illustrates the usability of this test bed. The Mica2 Motes have some indicators which have been used to simulate this type of attack. Each mote has three lights: red, green, and yellow. These lights have been used in this paper to simplify the demonstration of this solution such as showing how packets are traveling from one mote to another and showing when and how the wormhole attack happens. For example when the green light blinks, it means that the mote is sending a packet. The red light indicates that the mote has received a RREQ packet from other motes. The yellow light turns on when the mote has received a RREP packet from other motes. The green and yellow lights together indicate that a RREQ or RREP has been received at the destination. It is clear to say that the red light will be seen before the yellow light since the request packet comes before the reply. However, if the yellow light has been seen before the green light, it means a wormhole attack has been detected. The reason for this is the replay comes before or faster than the request packet. By doing this, it is easier now to understand what is happening during the demonstration.

3.5 Visibility of the test bed

There are two situations to run the test bed. The first situation is demonstrating the customized AODV routing algorithm without implementing the wormhole attacks. In other words, demonstrating customized AODV without the Stargate sensor devices. The second situation is demonstrating wormhole attack beside the customized AODV.

To demonstrate the first situation, it is important to turn the Stargate sensor devices off. The wormhole attack will not occur in this situation. To start this demonstration, firstly turn on motes 2, 3, 4, and 7. Then, turn on the mote 1 which acts as the original source. Mote 1 will start sending RREQ packet by blinking its green light. This sending will be after synchronized with global clock. Mote 2 will receive the RREQ packet, turn on its red light, and forward this packet by blinking its green light. Mote 3 will do the same thing that mote 2 has done. Finally, mote 4 will receive the RREQ packet, turn on its red light and yellow light indicating that the RREQ has reached its

destination, and prepare the RREP packet. The same process will happen for RREP packet, but the difference is that each mote will turn on its yellow light on receiving the RREP packet. Finally, Mote 4 will turn on its red and yellow lights on receiving the RREP packet indicating that the RREP has reached its destination.

The other situation is demonstrating the wormhole attack by adding the two Stargate with their motes. Firstly, turn on all motes and Stargates except mote 1 which is the original source. Then, turn on mote 1 to start sending the RREQ packet. In this situation, mote 4 which is the original destination will receive the RREQ from mote 1 directly through the Stargate path since the WiFi path is faster than the radio path. This happens when Mote 5 receives the RREQ packet from mote 1 and sends it directly through the WiFi connection to the other Stargate. Mote 6 in the other Stargate will send this packet to mote 4 via its radio antenna. The RREQ packet will travel through the WiFi connection faster than the normal path which is through the intermediate motes 2 and 3. In this situation, mote 4 will think that mote 1 is its direct neighbor and it will turn on its red light and yellow light preparing for the RREP packet. Mote 4 will send the RREP packet which will be delivered through the WiFi connection between the two Stargates. Mote 1 will turn on its red and yellow lights when it receives the RREP packet. Also, mote 1 will think that mote 4 is its direct neighbor and this is how the wormhole attack happens. It is possible to display the information of the packets and the final routing table in mote 1 by using a PC. More details of how to perform that have been provided in Chapter 3.

There are a number of techniques to solve the wormhole attack in a wireless sensor network. In the next section, some of these techniques will be briefly described. The implementation of one of them will be explained in section 3.7.

3.6 Wormhole Attack Solution

To detect and deter the Wormhole attack, some solutions have been proposed in different papers such as [4,9,10]. One of them will be described in this section.

Hu et al. proposed a defense against the Wormhole attacks in WSN called packet leashes [4]. It is the only solution that is implemented in this paper. A leash is a

portion of information that is added to the packet to restrict its traveling distance or time. This solution consists of two types of leashes: geographic leashes and temporal leashes. Each of these types will be described briefly in this section and more details are available in [4].

A geographic leash detects and prevents the wormhole attack by ensuring that the sender and the receiver are within a specified distance. To do that, each node must know its location and be timely synchronized with other nodes. When the sender starts sending the packets, it stores its location and the sending timestamp in the packet. Then, the receiver will calculate its location and the receiving timestamp and compare them with the values in the packet. By doing that, the receiver can detect if the sender is within its distance or not, which will help detection and prevention of the wormhole attack. For more details of how the geographic leash is working refer to [4].

The other type of solution is a temporal leash. It detects and prevents the wormhole attack by ensuring that the packet's traveling time is within a specified period of time. To do that, all nodes must be timely synchronized in terms of their clocks. When the sender starts sending the packets, it stores its sending timestamp in the packet. Then, the receiver can compare its receiving timestamp with the value in the packet. Therefore, the receiver will be able to detect if the packet traveled so fast according to a specified transmission time. For more details of how the temporal leash is working refer to [4].

In this test bed, the temporal leash solution has been used and implemented to detect and prevent the wormhole attack in the wireless sensor network. The geographic leash solution has not been considered in this paper because it is complicated to be implemented. It needs a special hardware that can specify the locations of all nodes such as GPS, which is expensive.

3.7 The Implementation of the 'Packet Leashes Solutions'

As it has been discussed earlier, timing mechanism is required to distinguish if the packet received from the fake path or the real path to avoid the wormhole attack. A packet received from the Stargate is going to be faster than the packet received from the mote

since the WiFi transmission is faster than the radio transmission. Therefore, applying this timing mechanism will allow the destination to recognize the real packet by comparing its time stamp with the time stamp of the received packet. If the difference between these two time stamps is less than or equal to X , it means that it is a fake packet. To compute the value of X according to the test bed design:

- There is a transmission delay in each mote. The average transmission delay is around 45 msec ($T_r = 45 \text{ msec}$). [5].
- The real path consists of mote 1, 2, 3, and 4 where the fake path consists of mote 1, 5, 6, and 4.
- Processing time at each mote will be neglected since both paths have the same number of motes. Therefore, the total processing time for motes in each path will be almost same.
- The WiFi transmission delay is neglected since the data rate is high.

Delay on the real path:

$$\begin{aligned} &= \text{No. of motes that will transmit} * T_r \\ &= 3 (\text{mote 1, 2, and 3}) * 45 \\ &= 3 T_r. \end{aligned}$$

Delay on the fake path:

$$\begin{aligned} &= \text{No. of motes that will do transmission} * T_r \\ &= 2 (\text{mote 1, and 6}) * 45 \\ &= 2 T_r. \end{aligned}$$

Therefore, the destination node is able to distinguish between the real and the fake packet by subtracting the time stamp at destination by the time stamp at the source. If the result $\leq 2 T_r$, then the packet is fake. Otherwise, it is real.

3.8 Difficulties

Unfortunately, synchronization cannot be applied at this stage since there is no clock implemented in the mote. Consequently, a global clock has been implemented to send the current time periodically to the other motes. Then, motes will update their local time according to what they have received. In this way, synchronize all motes with the global clock can be achieved. Then, the timing mechanism can be applied.

However, there is still a scenario where a wormhole attack can not be detected especially if the

environment is not reliable and some clock packets might be dropped. As been known, there are four clocks between the sender and receiver in the real path where three clocks only in the fake path. Therefore, if the destination dropped the fourth clock packet, the local time at the destination will be three clocks. Therefore, the difference between the time stamp at destination and sender will be just two clocks. This means, the destination will drop the packet assuming it is a fake packet according to the formula above.

4. Conclusion and Work future

The rapid development in the wireless sensor networks field has allowed this technology to be used in many applications. Some of these applications are critical and require secure and trusted environment. Therefore, different research studies have been conducted to analyze the wireless sensor networks and discovering their threats. One of the attacks which may damage wireless sensor networks is the Wormhole attack. Thus, this project tried to build a test bed of a group of sensor devices to simulate the wormhole attack and implement one of the solutions to detect and prevent this attack.

This report has explained what has been performed in this project. First, a brief background about the used sensor devices has been given such as MICA2 motes and Stargate. Then, it has explained the design and the implementation of the test bed by describing the proposed network topology, the algorithms, and the chosen solution. Finally, detailed steps of setting up the environment of all devices used in this project have been illustrated. In future, the timing mechanism that has been used might be improved especially with the new version of TinyOS that give the opportunity to implement internal clock in the mote. Also, this project could be enhanced by some additional improvements. One of these improvements is to apply this test bed on a large wireless sensor network. Moreover, different solutions for the wormhole attacks could be implemented and evaluated.

Acknowledgement

The authors would like to acknowledge Dr. Wen Hu, CSE, UNSW for his support with setting environment for TinyOS, Mica2, and Stargae. Also, the authors would like to acknowledge Manal Alfaraj, Griffith University for the early discussions.

5. References

- [1] Crossbow Technology, Inc., MPR/MIB Mote Hardware Users Manual, http://www.xbow.com/Support/Support_pdf_files/MPR-MIB_Series_Users_Manual.pdf
- [2] Crossbow Technology, Inc., Stargate Developer's Manual, http://www.xbow.com/Support/Support_pdf_files/Stargate_Manual.pdf
- [3] Ganeriwal, S., Kumar, R., & Srivastava, M.B. "Timing-sync protocol for sensor networks," ACM Conference on Embedded Networked Sensor Systems (SENSYS 2003).
- [4] Hu, Y., Perrig, A., & Johnson, D.B. "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), vol. 3, pp. 1976-1986, IEEE, San Francisco, CA, April 2003.
- [5] Paek, J., Chintalapudi, K., & Govindan, R. "A Wireless Sensor Network for Structural Health Monitoring: Performance and Experience" 2005.
- [6] Stargate Mailing List, <http://www.cens.ucla.edu/pipermail/stargate-users>
- [7] TinyOS website, <http://www.tinyos.net/>
- [8] TinyOS Mailing List, <http://www.tinyos.net/search.html>
<http://www.cens.ucla.edu/pipermail/stargate-user/>
- [9] Lazos, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W., "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," Wireless Communications and Networking Conference, 2005 IEEE , vol.2, no., pp. 1193-1199 Vol. 2, 13-17 March 2005.
- [10] Khalil, I.; Saurabh Bagchi; Shroff, N.B., "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, vol., no., pp. 612-621, 28 June-1 July 2005.

Study of Timing Values in EAP Authenticated Wireless Hosts

Janaka Silva, Elankayer Sithirasanen, and
Vallipuram Muthukkumarasamy

School of Information and Communication Technology
Griffith University, Gold Coast, Australia
j.silva@griffith.edu.au e.sithirasanen@griffith.edu.au
v.muthu@griffith.edu.au

Abstract. Wireless Local Area Networks have exhibited significant growth within the last few years in both home and corporate environments because of low cost and improved quality. This growth has fueled new applications for wireless networks ranging from advanced warehouse inventory systems to wireless Voice Over Internet Protocol (VoIP) phones. Sometimes the deployment of wireless local area networks (WLANs) is even more economical than installing wired networks in a building. However, the level of security of wireless and wired networks remain a major concern. The IEEE 802.11i standard together with IEEE 802.1X standard provide enhanced encryption and authentication mechanism enabling rigid security for the wireless networks. However, increasing wireless network security breaches has proven the lack of protection mechanism for the WLANs. In this context we propose to investigate the possibility of using round trip timing values for studying the behavior of wireless hosts under different abnormal conditions. In order to test our concept we have analyzed large number of traces captured using EAP, PEAP, LEAP and TLS authenticated hosts from our experimental wireless network environment.

1 Introduction

Security and the behavioral nature of the wireless environment is much more complex than wired environment. Normal behavior of a wireless network can change dramatically due to a number of reasons, including the inherent qualities of the wireless environment. Much research has been carried out to model the actual changes of the wireless networks. Most of them focus on the security issues of the wireless networks. The latest standard IEEE 802.11i [9] is developed to enhanced the security capabilities of the WLAN.

IEEE 802.11i defines security and mutual authentication mechanisms at the Media Access Control (MAC) layer. This standard is designed to address the security deficiencies in the Wired Equivalent Privacy (WEP) mechanism. IEEE 802.11i scheme uses strong encryption and other enhancements to improve security of the WLANs addressing three main security areas. It provides mutual

authentication, key management and data transfer privacy. On the assumption of upgrading the hardware, 802.11i defines CCMP that provides strong confidentiality, integrity and replay protection. The 802.11i architecture contains the following components: IEEE 802.1X [10] for authentication (enabling the use of EAP and an authentication server), Robust Security Network (RSN) for tracking associations and Advanced Encryption Standard, based on CCMP to provide confidentiality, integrity and origin authentication.

Although the IEEE 802.11i provides effective measures to protect the wireless networks from confidentiality and integrity threats, their reliance on authenticity and availability are still of major concern. On the other hand Intrusion Detection Systems (IDS) are used for detecting security breaches in wired as well as wireless networks. Huge amount of wireless traces can be collected from today's wireless network environment. Analyzing them may reveal vital information about the behavior of wireless hosts. One of the major challenges in wireless networks is to identify and differentiate the legitimate and non-legitimate wireless hosts. In this study we discuss the use of round trip timing (RTT) values, to detect unusual behaviors of the wireless hosts. As such we have demonstrated the RTT variations of EAP [5] LEAP [11], PEAP [14] and TLS [1] authenticated wireless hosts during RSN association process.

This report is organized as follows: In section 2 we give a brief summary of the various studies carried out related to anomaly detection. Section 3 we discuss the IEEE 802.11i RSN association process. Details of the experimental setup and the software model used for calculating the timing values are discussed in section 4. Results and analysis of the RTT values for EAP LEAP, PEAP and TLS authenticated hosts during normal and abnormal conditions are presented in section 5. Finally, section 6 concludes our paper.

2 Related Work

Analysis of IEEE 802.11i by Sithirasenan et. al. [16] identifies a number of weaknesses in the standard together with some solutions from the software implementation perspectives. A similar analysis by He et. al [7] on IEEE 802.11i wireless networking further highlights the weaknesses of the standard. They have discussed the possibilities of several attacks on poorly configured 802.11i networks. Further, they state that although the new security standard offers sufficient protection to the wireless environment it is up to the implementer to ensure that all issues are addressed and the appropriate security measures are deployed. For instance, a single misconfigured station could lead the way for a cowardly attack and expose the organizational network. Lynn et. al. [13] discuss that if no authentication mechanisms are implemented an adversary could establish two separate connections to the supplicant and the authenticator to construct a Man-in-the-Middle (MitM) attack. Furthermore, if mutual authentication mechanism is not appropriately implemented an adversary will be able to launch a MitM attack and learn the Pairwise Master Key (PMK) as illustrated by Asokan et. al. [4]. Although these vulnerabilities are not directly connected with 802.11i,

any implementer of 802.11i needs to consider these problems warily and keep monitoring the wireless hosts to guarantee proper integration of the security mechanisms.

Lim et al. [12] introduced a low cost solution for intrusion detection and response. Their system detects intrusions by various means such as MAC address filtering, tracking RTS/CTS to detect passive intruders and stateful monitoring to detect random responses by intruders. The prototype developed had several limitations in the processing power, hence the authors focused only on selected intrusions. They mainly considered DoS attacks and their system detected the NetStumbler without any false positives.

Gill et al. [6] proposed a passive technique for detecting session hijacking attacks. They use Received Signal Strength (RSS) and Round Trip Timings (RTT) to detect anomalies. Both cases require frequent re-tuning of threshold values for satisfactory performance. However, their system cannot be extended to detect other security threats in the wireless environment.

In addition to the above techniques there are several commercial products used for intrusion detection and preventions. AirDefence [2] and Air Magnet [3] claim to provide a complete hardware and software solution for intrusion detection and prevention in 802.11 wireless networks. AirDefence detects intruders and attacks and also analyzes vulnerabilities. Although the manufacturers claim their system provides active responses to every possible intrusion attempts there is no statistical evidence to justify it. Furthermore, WLANs with 802.1x authentication are yet to become popular and hence the credibility of the commercial systems still needs to be verified.

In a further study by Sithirasenan et al. [15] they discuss the use of different characteristics of the WLANs to substantiate between legitimate and illegitimate hosts. In their study they have proposed a system to monitor both timing and behavioral anomalies and the use a outlier based data association technique to substantiate the anomaly. They collected large amount of network traces, stored and analyzed them in order to detect and distinguish real time attacks on the wireless environment. For real time intrusion detection and prevention they have proposed a robust system called Early warning System (EWS). As an extension to the timing anomaly studies, in this paper we investigate the RTT values of EAP LEAP, PEAP and TLS authenticated hosts under both normal and abnormal conditions

3 Robust Security Network

The IEEE 802.11i standard defines two classes of security framework for IEEE 802.11 WLANs: RSN (Robust Security Network) and pre-RSN. A station is called RSN capable equipment if it is capable of creating RSN Associations (RSNA), otherwise, it is a pre-RSN equipment. In an Extended Service Set (ESS), during the RSNA a number of messages are exchanged between the supplicant (STA) and the authenticator (AP). The network that only allows RSNA with RSN-capable equipments is called a RSN security framework. The major

difference between RSNA and pre-RSNA is the 4-way handshake. If the 4-way handshake is not included in the authentication / association procedures, stations are said to use pre-RSNA.

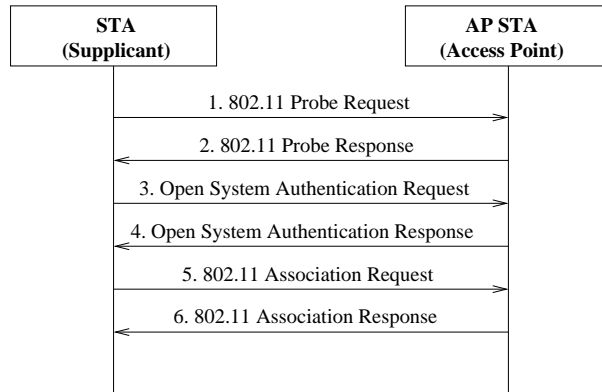


Fig. 1. RSN Discovery Phase

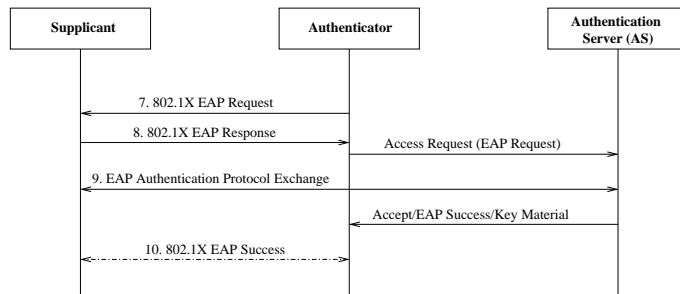


Fig. 2. RSN Authentication Phase

Figure 1 shows the first phase in RSNA - the discovery phase. During this phase both the STA and the AP agree on a common security policy. Flows 1-6 are the IEEE 802.11 [8] association process prior to attaching to the AP. During this process, security information and capabilities are negotiated using the RSN Information Element (IE). The Authentication in flows 3 and 4 refer to the IEEE 802.11 open system authentication. On successful completion of the discovery phase the AP initiates the authentication phase by starting the IEEE 802.1X [10] authentication as shown in Figure 2. If the STA and the authentication server authenticate each other successfully, both of them independently generate a Pairwise Master Key (PMK). Depending on the type of authentica-

tion mutually agreed between the STA and the authentication server, there could be several messages exchanged between them (flow 9) before the PMK is generated. The authentication server then transmits the PMK to the AP through a secure channel (for example, IPsec or TLS).

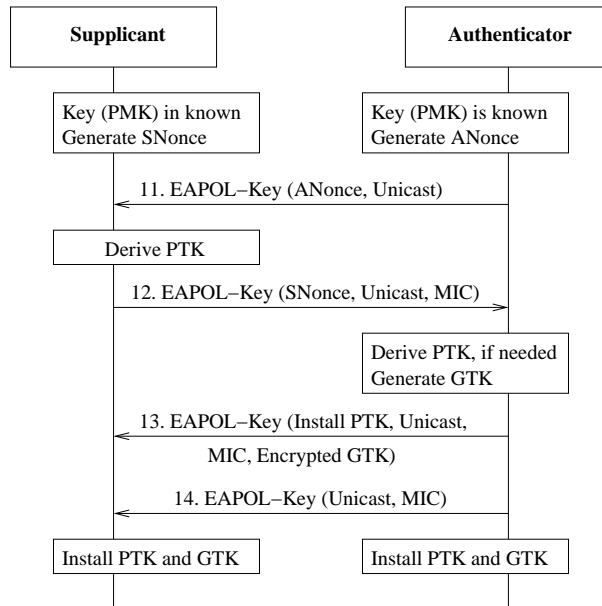


Fig. 3. RSN Key Establishment Phase

The next phase in the RSNA is the key distribution phase as illustrated in Figure 3. The PMK generated during the authentication phase is used to derive and verify a Pairwise Transient Key (PTK), guaranteeing fresh session key between the STA and the AP. This is called the 4-way handshake phase as shown by flows 11 - 14. Next, the group key handshake is initiated. The group key handshake is used to generate and refresh the Groupwise Transient Key (GTK), which is shared between a group of STAs and APs. Using this key, broadcast and multi-cast messages are securely exchanged in the air.

Considering the RSN messages discussed above, in this paper we have analyzed the significance of RTT values for detecting anomalies. We have studied the RTT behavior of wireless hosts configured for EAP LEAP, PEAP and TLS authentication during their RSN association. In the next section we present the RTT values of the wireless hosts during normal conditions.

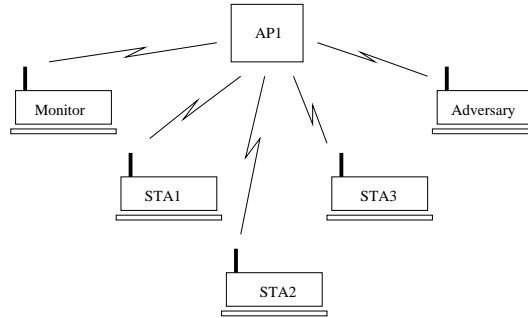


Fig. 4. Test Wireless Environment

4 Experiments

The experimental setup as shown in Figure 4 has a single Access Point (AP) and several wireless stations (STA) configured to authenticated with the AP using the different EAP authentication mechanisms. Here, STA1 and STA2 are both Linux machines and STA3 is a Windows XP machine. STA1 is configured for EAP-LEAP authentication, STA2 is configured for EAP-PEAP authentication and STA3 for EAP-TLS authentication. The Monitor is part of the data processing unit which captures wireless network traffic in promiscuous mode. The Adversary is capable of introducing various anomalies into the wireless network. When the experiments were carried out the test setup was exposed to the normal wireless environment of the university attracting traffic from various unspecified sources. Using this setup large number of wireless traces were collected and analyzed.

The software model for storing and calculating the timing values was built using PHP and MySQL. Basically the model takes the wireless traces as an input, processes it and stores them in a database table. Once the traces are stored in the database in a predefined format, the model queries the database and takes each of the EAP type traces separately and processes them and stores the RTT values together with various statistical information in another database table. One separate result table is used for one EAP Type method, for example if we want EAP TLS timing profile table we can generate it dynamically after the traces were stored in the database. The following pseudo code describes the derivation of the various statistical values from the database tables.

```

$result1 = query EAP specific Association Request Events from STA to AP
$result2 = query EAP specific Association Response Events from AP to STA
$rttsum = 0
$rttcount = 0
  
```

```

while more rows in $result1
  fetch the next row in $result1 into $row1
  fetch the next row in $result2 into $row2

  while $row1 timing value > $row2 timing value
    fetch the next row in $result2 into $row2
  end while
end while
  
```

```

        calculate current RTT value
        store current RTT value if it is the Maximum
        store current RTT value if it is the Minimum
        add current RTT value to $rttsum
        add one to $rttcount
    end while
calculate Average RTT
calculate Standard Deviation for RTT

```

The output RTT values table is defined based on each of the events associated with the respective EAP type. The timing profiles in these tables are the timing values to complete a particular round trip event during each of the EAP type specific authentication process. In this context a round trip event is considered to be the completion of two messages. The Request sent by the AP or STA and corresponding response received by the AP or STA. In order to present the values in a more functional manner the Mean, Maximum, Minimum, Standard deviation and the number of request and responses are calculated dynamically and stored. The Mean, Maximum and Minimum timing values together with the standard deviation gives the range of timings allowed for the round trip events during the normal operations.

5 Results and Analysis

Firstly, we present the measured RTT values of EAP LEAP, PEAP and TLS authenticated hosts during the RSN association process, under normal operations. In section 5.2, we present the RTT values of the these hosts under abnormal conditions from our experiments.

5.1 Normal behavior

Event	Min (ms)	Max (ms)	Mean (ms)	StDev
OPEN AUTHENTICATION	0.08	3.40	0.61	0.53
OPEN ASSOCIATION	0.51	2.65	0.65	0.29
EAP 1	0.05	2.57	0.79	0.43
EAP 2 (PEAP)	0.03	1.55	0.35	0.21
EAP 3 (LEAP)	0.42	1.30	0.48	0.13
EAP 4 (LEAP)	3.05	9.77	3.32	0.89
EAP Key Exchange	0.07	11.36	2.54	2.16
Overall	12.81	321.97	18.96	37.06

Table 1. EAP-LEAP Timing Profile

Table 1 shows the EAP-LEAP RTT values between AP1 and station STA1 obtained from a trace file consisting more than one hundred EAP-LEAP RSN associations, under normal conditions. The timing profile shows the allowable timing range required to complete a particular round trip event during normal EAP-LEAP authentication process. In this case, there are a total of seven

EAP-LEAP request/response messages. The maximum, minimum, mean and standard deviation values were calculated by the software model. This gives us an indication of the possible range of RTT values during the normal operations.

Event	Min (ms)	Max (ms)	Mean (ms)	StDev
OPEN AUTHENTICATION	0.37	0.61	0.44	0.05
OPEN ASSOCIATION	0.55	1.41	0.61	0.10
EAP 1	0.10	2.03	0.57	0.46
EAP 2 (PEAP)	0.23	4.24	2.05	0.80
EAP 3 (PEAP)	0.08	1.76	0.40	0.21
EAP 4 (PEAP)	0.02	1.49	0.83	0.41
EAP 5 (PEAP)	0.58	1.08	0.62	0.06
EAP 6 (PEAP)	0.36	0.59	0.45	0.03
EAP 7 (PEAP)	0.72	4.29	2.70	0.51
EAP 8 (PEAP)	0.08	2.50	0.60	0.44
EAP 9 (PEAP)	0.18	1.65	0.50	0.28
EAP Key Exchange	0.05	7.68	1.62	1.22
Overall	48.65	68.09	52.25	3.78

Table 2. EAP-PEAP Timing Profile

Table 2 shows the EAP-PEAP RTT values between AP1 and station STA2, obtained from a trace file consisting more than one hundred EAP-TLS RSN associations, under normal conditions. The timing profile shows the allowable timing range required to complete a particular round trip event during normal EAP-PEAP authentication process. Unlike for EAP-LEAP authentication, EAP-PEAP involves a total of twelve EAP-PEAP request/response messages.

Event	Min (ms)	Max (ms)	Mean (ms)	StDev
OPEN AUTHENTICATION	0.37	3.57	0.56	0.51
OPEN ASSOCIATION	0.11	9.07	0.85	0.85
EAP 1	36.25	106.13	53.91	8.24
EAP 2	10.89	89.74	25.69	11.11
EAP 3 (PEAP)	0.71	17.72	4.01	4.41
EAP 4 (TLS)	6.56	56.55	43.89	10.98
EAP 5 (TLS)	0.08	43.39	4.63	9.04
EAP 6 (TLS)	13.66	71.68	17.83	8.16
EAP 7 (TLS)	0.738	39.41	4.36	5.01
EAP Key Exchange	1.74	76.21	22.67	20.27
Overall	134.45	244.30	162.74	17.41

Table 3. EAP-TLS Timing Profile

Table 3 shows the EAP-TLS RTT values between AP1 and station STA3, obtained from a trace file consisting more than one hundred EAP-TLS RSN associations, under normal conditions. The timing profile shows the allowable timing range required to complete a particular round trip event during normal EAP-TLS authentication process. In this context a round trip event is considered to be the competition of two messages; a request and the corresponding response.

By approximating the RTT values to a standard normal distribution, we can specify an upper and a lower limit for RTT values (with one standard deviation above and below the mean value) of each EAP event. For example, in the case of EAP-TLS authentication, the lower limit of the overall RTT value would be 145.33 ms and the upper limit would be 180.15 ms. We can use these values as typical for timing anomaly detection.

5.2 Abnormal Conditions

Above discussed RTT profiles represent for normal behavior of EAP authenticated hosts. However when anomalies occur this behavior can change. There can be situations where the numbers of events are extraordinary high or low. There can also be situations where events can totally disappear from the respective range of the monitoring devices. Furthermore, abnormalities can be due to various wireless security attacks, such as, DoS, Man-in-the-Middle attack, Replay Attacks etc. Other reasons may be environmental disturbances. Since we are using IEEE 802.11 WLAN which operates on 2.4 GHz frequency band, it has higher probability of attracting noise and interferences. WLAN characteristics can vary widely, depending on device characteristics (e.g. antenna design and orientation) and environmental factors (e.g. floor plan). Following are some observations obtained during the abnormal conditions.

Event	Time (ms)
OPEN AUTHENTICATION	6.22
OPEN ASSOCIATION	4.28
EAP 1	6.11
EAP 2 (PEAP)	4.15
EAP 3 (LEAP)	3.27
EAP 4 (LEAP)	12.92
EAP Key Exchange	16.19
Overall	996.44

Table 4. Abnormal EAP-LEAP Timings

Table 4 is a good example of abnormal RTT values. These values are the average of more than ten experiments carried out by injecting abnormal management frames with EAP-LEAP authenticated hosts. According to these EAP-LEAP RTT values, almost every message exchange show significantly high RTT values resulting in high overall timing, compared with the normal values in Table 1. Also it can be seen that the timing values of every message exchange are highly unpredictable. Furthermore, statistically we can conclude that these timing values are abnormal since they do not fall within the 68% of the standard normal distribution. Figure 5 shows the mean and one standard deviation from mean values of EAP-LEAP RTT timings together with abnormal RTT values.

Table 5 shows another set of RTT values for EAP-PEAP authenticated hosts. These values are the average of more than ten experiments carried out by inject-

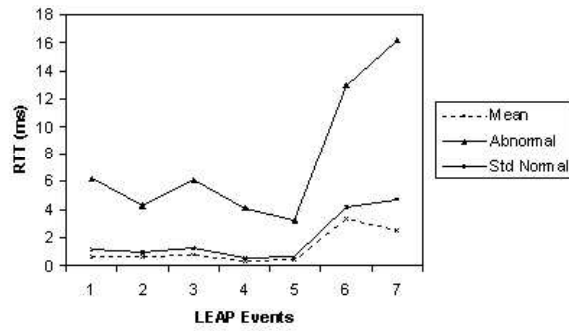


Fig. 5. EAP-LEAP Timings

Event	Time (ms)
OPEN AUTHENTICATION	8.26
OPEN ASSOCIATION	7.10
EAP 1	8.85
EAP 2 (PEAP)	6.07
EAP 3 (PEAP)	7.11
EAP 4 (PEAP)	12.47
EAP 5 (PEAP)	8.45
EAP 6 (PEAP)	11.99
EAP 7 (PEAP)	5.87
EAP 8 (PEAP)	9.64
EAP 9 (PEAP)	7.91
EAP Key Exchange	6.68
Overall	628.40

Table 5. Abnormal EAP-PEAP Timings

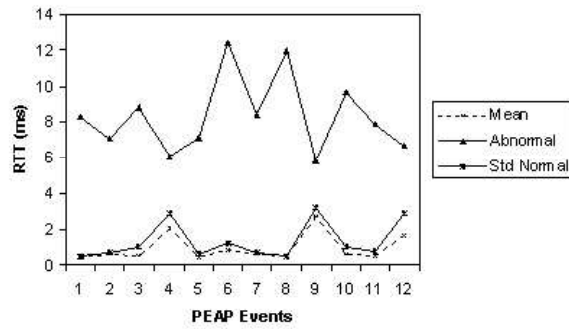


Fig. 6. EAP-PEAP Timings

ing abnormal management frames with EAP-PEAP authenticated hosts. Statistically, it is evident that most of the RTT values do not fall within the 68% of the standard normal distribution. Also, the first three RTT values are considerably high compared to the others. This is due to the unpredictable nature of the Open System association process, where hosts can be made to repeatedly deauthenticate and re-associate. The *zscore* (the number of standard deviations away from the mean) for the overall timing value is 150 in this case. Figure 6 shows the mean and one standard deviation from mean values of EAP-PEAP RTT timings together with abnormal RTT values.

Event	Time (ms)
OPEN AUTHENTICATION	3.07
OPEN ASSOCIATION	78.47
EAP 1	79.17
EAP 2	120.36
EAP 3 (PEAP)	16.11
EAP 4 (TLS)	89.24
EAP 5 (TLS)	25.26
EAP 6 (TLS)	33.21
EAP 7 (TLS)	44.75
EAP Key Exchange	35.69
Overall	1140.15

Table 6. Abnormal EAP-TLS Timings

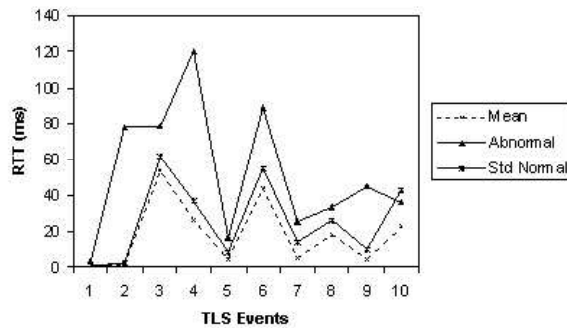


Fig. 7. EAP-TLS Timings

The RTT values shown in Table 6 can be considered as abnormal since the timing values for the EAP-TLS Request/Response messages are significantly high resulting in a high overall timing. These RTT values also do not fall within the 68% of the normal standard distribution. As we can see from Table 3 the normal RTT values, except for authentication and key exchange messages all

other messages do not lie within the acceptable deviation range and do not fall within standard normal distribution. In this case the *zscore* for the overall timing value is 56. Figure 7 shows the mean and one standard deviation from mean values of EAP-TLS RTT timings together with abnormal RTT values.

As seen in figures 5, 6 and 7 the mean RTT values for EAP-LEAP, PEAP, and TLS authenticated hosts are very much less than the abnormal RTT values. The three graphs can be used to visualize the significant differences between normal RTTs and abnormal RTTs for each event. Throughout our experiment we assumed that the calculated RTTs (using sample wireless traces) behave according to the normal distribution. Also RTT of a message exchange is a passive detection mechanism to detect unusual behaviors of the wireless as well as wired networks. Hence this technique may be used to detect intruders who can adversely affect the wireless network environment.

However this particular study does not address any specific type of wireless attacks. RTT measures can be used effectively in wireless networks if it is combined with appropriate statistical methods. In our future studies we will use two different statistical methods, namely t-test and Chi-square test to investigate the RTT values during different attack scenarios.

6 Conclusions

This study was conducted to investigate the characteristics of normal and abnormal RTT values of EAP-TLS, PEAP and LEAP authenticated wireless hosts. In this view we have presented a comparison between the normal and abnormal RTT values. The statistical timing values show that there is a significant variation between the values for normal and abnormal associations. This type of timing analysis may be useful to find out abnormalities in the wireless environment and may be helpful for wireless network intrusion detection and prevention.

In future work we will extend this research to find the best possible statistical representation for RTT values in various situations for a number of EAP type specific authentication methods. With more appropriate statistical representation we expect better intrusion detection and prevention capabilities.

References

1. B. Aboba and D. Simon. PPP EAP TLS Authentication Protocol. <http://tools.ietf.org/wg/pppext/draft-ietf-pppext-eaptls/draft-ietf-pppext-eaptls-06.txt>, August 1999.
2. AirDefence - intrusion protection and monitoring. <http://www.airdefense.net/products/enterprise.php>. Cited March 2006.
3. AirMagnet - wireless network management systems. <http://www.airmagnet.com/products/enterprise.htm>. Cited March 2006.
4. N. Asokan, V. Niemi, and K. Nyberg. Man-in-the-Middle in tunneled authentication protocols. Technical Report 2002/163, IACR ePrint archive, United Kingdom, October 2002.

5. L. Blunch and J. Vollbrecht. Extensible Authentication Protocol (EAP). <http://www.ietf.org/rfc/rfc2284.txt>, March 1998.
6. R. Gill, J. Smith, M. Looi, and A. Clark. Passive technique for detecting session hijacking attacks in IEEE 802.11 wireless networks. In *AusCERT '05: Proceedings of the 4th Asia Pacific Information Technology Security Conference*, pages 26–38, May 2005.
7. C. He and J. C. Mitchell. Security Analysis and Improvements for IEEE 802.11i. In *Proceedings of the 12th Annual Network and Distributed System Security Symposium*, February 2005.
8. IEEE Standard 802.11. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, June 1999.
9. IEEE Standard 802.11i Part 11. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements*, July 2004.
10. IEEE Standard 802.1X. *Local and Metropolitan Area Networks, Port-Based Network Access Control*, June 2001.
11. C. S. Inc. Cisco LEAP (LEAP). <http://ietfreport.isoc.org/all-ids/draft-josefsson-pppext-eap-tls-eap-07.txt>, October 2003.
12. Y. Lim, T. Schmoyer, J. Levine, and H. Owen. Wireless intrusion detection and response. In *Proceedings of the IEEE Systems, Man and Cybernetics Society Information Assurance Workshop*, volume 18, pages 68–75, June 2003.
13. M. Lynn and R. Baird. Advanced 802.11 attack., July 2002.
14. A. Palekar, D. Simon, G. Zorn, J. Salowey, H. Zhou, and S. Josefsson. Protected EAP Protocol (PEAP). <http://ietfreport.isoc.org/all-ids/draft-josefsson-pppext-eap-tls-eap-07.txt>, October 2003.
15. E. Sithirasenan and V. Muthukkumarasamy. Substantiating Security Threats Using Different Views of Wireless Network Traces. In *AusCERT'07: Proceedings of the 6th Asia Pacific Information Technology Security Conference*, pages 31–49, May 2007.
16. E. Sithirasenan, S. Zafar, and V. Muthukkumarasamy. Formal Verification of the IEEE 802.11i WLAN Security Protocol. In *ASWEC'06: Proceedings of the 21st Australian Software Engineering Conference*, pages 181–190, April 2006.

APPENDICES:

- A. AusCERT 2008 “*SETMAPE*“ Stream call for papers.

Appendix A:



CALL FOR PAPERS

**AusCERT Conference 2008:
R&D Stream
SETMAPE**

**“Science, Engineering, Technology,
Mathematics, Policy and Education”
Stream**

Tuesday 20 May 2008.
Crowne Plaza Royal Pines Resort
Gold Coast, Queensland. Australia.

NEW CLOSING DATE FOR PAPER SUBMISSION: 5.00PM Monday 5 May 2008.

The R&D (SETMAPE) Stream at AusCERT-2008

Professional and managerial practice in all aspects of information security and assurance is underpinned by some basic propositions of integrity, confidentiality, availability, trust, recovery and the like. These propositions are themselves governed by the scientific, engineering, technological, mathematical, policy and education fundamentals that build that required trust and confidence in global information systems. However, this must be set against a thorough understanding of the risks involved involving the combination of vulnerabilities, threats and perceived consequences of system failure for whatever reason. This stream augments the broad themes of AusCERT by making a place for exposition of underlying research and development activities in the area and builds upon the success of previous research oriented streams at the AusCERT conferences.

The basic aspects of overall information system assurance are continuously improved and clarified through all aspects of research and development activity, ranging from analysis of the most fundamental aspects of mathematical cryptology to the construction and testing of secure computer systems and vulnerability identification to the creation and analysis of vital information security policy and human factor analysis. Coupled with all this is, of course, the need to better understand how such R&D can best be used for the betterment of assurance in critical information systems through advances in the development and practice of education and training in the area as well as in public policy development and legal practice.

The SETMAPE stream at AusCERT aims at bringing together researchers and developers with those involved in the practical day-to-day aspects of managing the security of real information systems in both the public and private sectors. It is an opportunity for

practitioners to offer feedback to the R&D community, to expound on the needs in the real world and, in turn, to for academic and industry researchers and teachers to relate R&D to actual requirements and management realities.

Papers in the SETMAPE stream are particularly aimed at explaining research and development efforts with an emphasis on associated results and their implications.

SETMAPE Time and Location

The 2008 AusCERT conference will take place from:

Sunday 18th to Friday 23rd May 2008 at the
Crowne Plaza Royal Pines Resort, Gold Coast, Australia.

The SETMAPE stream of the conference will be held on **Tuesday 20 May 2008** at the conference venue which is detailed on the main AusCERT 2008 conference website.

Thus papers and presentations based on research, development, policy and education/training aspects of the broader topics to be covered in the main conference are sought. These topics can be viewed at the AusCERT 2008 main website at URL <http://www.auscert.org.au> In addition to those topics the following areas may also be covered:

- Protecting the national information infrastructure: policy and process research
- Politics of information security
- Research into legal aspects of information systems security, including “e-discovery”, liability, etc.
- Employee attitudes and responses to information systems security
- Advances in automation of risk assessment and management methodologies
- Use and integration of encryption technologies, as well as security of these sub-systems, including use of the “trusted platform module (TPM)”
- Network security protocols and their evaluation
- Security in a “Web 2.0” application development and deployment environment
- Malware detection and eradication at the hardware, OS kernel, device driver and other levels
- New paradigms in access control for the network, operating system, database and application
- Security of SCADA/DCS systems
- Security in specific systems environments, including Microsoft Windows and LINUX
- Database management system security
- Security in a Wireless Environment
- Information security education and training
- Security in the e-health environment
- Trusted systems research and development, including SELinux, etc.
- Reverse engineering for information security and cryptographic subsystem assessment

Publication of Papers:

For those wishing to submit papers it should be noted that all papers will be blind refereed by an expert program committee and selected papers will be published in the formal proceedings of the stream which will be in electronic format only.

(For Australian academic authors this should mean that papers will normally fit under the E1 category for research credit purposes.)

Deadlines (Extended Closing Date – 5 May 2008.):

Draft papers must be forwarded to the AusCERT secretariat by 17.00hrs (5.00pm) on **Monday 5 May 2008**. Authors of successful papers will be notified within 4 days as to the acceptance of a submitted paper. Final papers, with any corrections, are then due 7 days from that date.

Submission Details:

Send to address:

Papers should be electronically submitted in any reasonable format by email to:

Emeritus Prof William J Caelli, AO
Chair – Programme Committee

at the following address:

setmape08@auscert.org.au

or via the main AusCERT 2008 conference website at the following URL:

<https://www.auscert.org.au/callforpapers>

Paper Formats:

- File formats may include Adobe Acrobat “.pdf”, Microsoft Word “.doc”, Standardised “.rtf”, Postscript “.ps”, Open Document Format “.odf”, ASCII text “.txt”, Hypertext “.html” or any reasonable other format, with details to be supplied.
- Paper size should be set to standard A4 size with 2.5cm (1 inch) margins all around and the type font should be set to 12 point.
- No size limit is set given that papers in various basic discipline areas vary widely in size, e.g. scientific and mathematical papers versus those from research activity in the legal and public policy areas. However, a strict time limit for presentation of the paper at the SETMAPE stream will apply.
- In order to allow for blind referring of papers please ensure that:
 - The title of the paper,
 - The names, affiliations and contact points for the authorsare placed on a separate front page that may be removed.
- The paper title, abstract, keywords and the start of the main text should start on the second page.
- The usual formal requirements for paper layout as set out by the Australian Computer Society, IEEE or ACM for publication in their professional scientific/technological research archive publications should be followed. The appropriate details for the Australian Computer Society’s (ACS) “*Journal of Research and Practice in Information Technology*” are available at the following URL:
<http://www.acs.org.au/jrpit/JRPITAuthors.html>

Attendance at the AusCERT 2008 Conference and Presentation of Papers:

It is expected that the author, or one of the authors, of the paper will attend at least the SETMAPE day of the AusCERT 2008 conference on the Gold Coast. In this case a single day SETMAPE conference fee, if required, for the AusCERT 2008 conference **will be waived** for the presenting author.

Further Information:

If required, further information may be obtained from the AusCERT 2008 conference secretariat whose details are given on the main AusCERT website at URL:

<http://www.auscert.org.au>

The SETMAPE Program Committee:

Chair:

Emeritus Professor William J (Bill) Caelli, AO
Director
International Information Security Consultants Pty Ltd, and
Senior Research Scientist
Information Security Institute – Queensland University of Technology
Email: w.caelli@iisec.com.au
Phone: National 07 – 5502 2978 International: +61-7-5502 2978

Deputy Chair:

Professor Paul Bailes
Head, School of ITEE
The University of Queensland, Queensland. Australia
Email: p.bailes@uq.edu.au

Members:

Dr Cristina Cifuentes
Sun Labs Down Under
The University of Queensland
Email: cristina.cifuentes@sun.com

Dr Guido Governatori
School of Information Technology and Electrical Engineering
The University of Queensland
Email: guido@itee.uq.edu.au

Emeritus Professor Dennis Longley
Director
International Information Security Consultants Pty Ltd., Queensland, Australia
Email: d.longley@iisec.com.au

Dr Vallipuram Muthukumarasamy
School of Information and Communication Technology
Griffith University Gold Coast Campus

Email: v.muthu@griffith.edu.au

Dr Juanma Gonzalez Nieto
Research Fellow – Information Security Institute and
Faculty of Information Technology,
Queensland University of Technology
Email: juanma@isrc.qut.edu.au

Dr Marius Portmann
School of Information Technology & Electrical Engineering
The University of Queensland, Queensland, Australia
Email: m.portmann@uq.edu.au

Professor Corey D. Schou
University Professor of Informatics
Idaho State University, Idaho. USA.
Director, National Information Assurance Training and Education Center
Idaho. USA.
Email: schou@cob.isu.edu

Mr Luke Wildman
System Safety and Quality Engineering Pty Ltd
Email: luke@ssqe.com.au