secure mobile ad-hoc networks and sensors

presentation topics

Singapore .:. September 20-22, 2005

1001010100101001100010101010010010010101001111101001001101001001101100101010101110

Wednesday, 21 September 2005

10.00am ~ 11:00am

Welcome to MADNES'05.

Gligor, Virgil. DATAMAXX Group Keynote Address: "On the Security of Emergent Properties in Traditional and Ad-Hoc Networks."

11.20am ~ 12.50pm

Sadi, Mohammed, Jong Sou Park, Dong Seong Kim, & Young Deog Song. "A Novel Pairwise Key Predistribution scheme for Ubiquitous Sensor Network."

Secure communication is an open challenge for Ubiquitous Sensor Network (USN) collecting valuable information. Sensor nodes have highly constrained resources like limited battery power, memory, processing capabilities etc. These Limitations make infeasible to apply traditional key management techniques such as public key cryptography or other complex cryptographic techniques in the USN. Based on polynomial key pre-distribution protocol, we propose a novel key predistribution technique to establish a pairwise key between sensors. In our scheme, we adopt the Probabilistic Randomness concept on the basis of Grid Based Scheme in a way to achieve improved resil-iency over large number of node compromise compared to the existing key pre-distribution schemes. Beside substantial improved resiliency, it also provides high probability and efficiency in establishing pairwise keys both in direct or path discovery method. Security analysis shows the effectiveness of our scheme in terms of resiliency improvement with little additional overheads in memory and communication.

Sanchez, David, & Heribert Baldus. "Key Management for Mobile Sensor Networks."

Key management is paramount for mobile sensor network (MSN) security. The special nature of MSNs imposes challenging requirements on key management design. We evaluate current key management techniques proposed for wireless sensor networks in the context of MSNs and identify open issues for research. We also propose a novel approach to control and replace pool-based pre-distributed keys. The analysis in this paper shows that this approach keeps the initial connectivity and resiliency properties of the key pre-distribution scheme even when nodes and keys are revoked.

Chen, Yun, Reihaneh Safavi-Naini, & Joonsang Baek. "Server-Aided RSA Key Generation against Collusion Attack."

In order to generate RSA keys on low-power hand-held devices, server-aided RSA key generation protocols were proposed. One drawback of these protocols, however, is that they cannot prevent a "collusion attack" in which two key generation servers communicate with each other to get useful information about the user's private key. In this paper, we present two new server-aided RSA key generation protocols secure against such an attack. Fast primality test, locally running on a hand-held device, is adopted in our protocols. In addition, we offload part of computational overhead on hand-held to the server in the single server-aided key generation circumstance.

2.10pm ~ 4.10pm

McDonald, Jeffrey. "Hybrid Approach for Secure Mobile Agent Computations."

Mobile agent applications are particularly vulnerable to malicious parties and thus require more stringent security measuresbenefiting greatly from schemes where cryptographic protocols are utilized. We review and analyze methods proposed for securing agent operations in the face of passive and active adversaries by means of secure multi-party computations. We examine the strengths and weaknesses of such techniques and pose hybrid schemes which reduce communication overhead and maintain flexibility in the application of particular protocols.

Navarro, Guillermo, & Joan Borrell. "Towards an Standards-based Authorization Framework for Mobile Agents."

An outstanding security problem in mobile agent systems is resource access control, or authorization in its broader sense. In this paper we present an authorization framework for mobile agents. The system takes as a base distributed RBAC policies allowing the discretionary delegation of authorizations. A solution is provided to assign authorizations to mobile agents in a safe manner. Mobile agents do not need to carry sensitive information such as private keys nor they have to perform sensitive cryptographic operations. The proposed framework makes extensive use of security standards, introducing XACML and SAML in mobile agent system. These are widely accepted standards currently used in Web Services and Grid.

Wright, Rebecca. Keynote: "Privacy-Preserving Datamining in the Fully Distributed Model."

4.30pm ~ 6.00pm

Kranakis, Evangelos, Jeyanthi Hall, & Michel Barbeau. Keynote: "Enhancing Intrusion Detection in Future Wireless and Mobile Networks."

We discuss approaches to enhancing intrusion detection in future wireless and mobile networks. We elaborate on approaches to incorporating radio frequency fingerprinting (RFF) into a wireless intrusion detection systems for detecting MAC spoofing. We examine the feasibility of using profiles, which are based on the mobility patterns of mobile users. We conclude with an examination of the security needs of forthcoming wireless and mobile systems.

Thursday, 22 September 2005

9.00am
~
11:00am

Krzywiecki, Lukasz, & Mirek Kutylowski. "Anonymous Distribution of Encryption Keys in Cellular Broadcast Systems."

We consider distribution of encryption keys for pay-per-view broadcasting systems with a dynamic set of users. We assume that the active recipients in such a system (i.e. those who pay for the current transmission) obtain a symmetric encryption key necessary for decoding the transmission. If the set of recipients changes, the system has to update the key and inform the legitimate users about the change. Communication medium we consider here is an ad hoc network of users organized in the same way as GSM or UMTS: the service area is divided into cells, each cell serves a limited number of users on its territory. Communication with the users in a cell is through a shared communication channel. We consider the problem of updating the encryption key when the set of users changes. We pursue three goals: communication volume related to a change of the encryption key should be kept as small as possible, the energy cost for each legitimate user should be low, the update process should not reveal any information about users behavior. We present a procedure for distributing a new key in environments where the set of users changes significantly. Our scheme is based on balanced allocation algorithms. The scheme is simple, easy to implement, and provides anonymity, small communication overhead and low energy cost for the users. The scheme works very well for a practical parameter size.

Jeon, Jun-Cheol, Kee-Won Kim, & Kee-Young Yoo. "Non-Group Cellular Automata based One Time Password Authentication Scheme in Wireless Networks."

Wireless network applications mostly authenticate clients with an identity / password or pin. OTP authentication schemes have developed based on time synchronization or one-way hash functions, although they can be trouble some and they have a high computational complexity. The current paper provides secure authentication for low-power wireless devices and other applications requiring authentication that is secure against passive attacks based on replaying captured and reusable passwords. In addition, our scheme highly minimizes the computational and transmission complexity and solves time or sequence synchronization problems by applying non-group cellular automata, based on the non-reversibility and uniqueness of the state configuration.

Zheng, Yuliang. Keynote: "Efficient Cryptographic Techniques for Mobile Ad-Hoc Networks."

11.20am
~
12.50pm

Lee, KyungKeun, JoonHyo Oh, & Sang-Jae Moon. "How to Generate Universally Verifiable Signatures in Ad-Hoc Networks."

This paper addresses the problem of making signatures of one domain (an ad-hoc network) available in another domain (the Internet). Universal verifiability is a highly desirable property when signed documents need to be permanently non-repudiable so as to prevent dishonest signers from disavowing signatures they have produced. As a practical solution, we construct a new signature scheme where a valid signature should be generated by a couple of distinct signing keys. In the random oracle model, the signature scheme is provably secure in the sense of existential unforgeability under adaptive chosen message attacks assuming the hardness of the computational Diffie-Hellman problem in the Gap Diffie-Hellman groups.

Li, Jun, Bruce Christianson, & Martin Loomes. "'Fair' Authentication in Pervasive Computing."

Authentication is traditionally required to be strong enough to distinguish legitimate entities from unauthorised entities, and always involves some form of proof of identity, directly or indirectly. Conventional storable or delegable authentication scenarios in the pervasive computing environment are often frustrated by the qualitative changes of pervasive computing when human are admitted into the loop. In this paper, we present an alternative approach based upon involving human self-determination in security protocols. This targets the authentication problem in pervasive computing, particularly when communication occurs in mobile ad-hoc fashion. We propose the argument of &quot;thinkable&quot; authentication, which involves using two-level protocols with the consideration of minimising trustworthiness in both human and computer device domains, but without unnecessary entity identity authentication. Thus, self-determining knowledge of the human interactions in pervasive computing can be exploited in order to make improvements on current security mechanisms.

Yunyi, Liu, Tuanfa Qin, Wansun Ni, & Shuyi Zhang. "Cryptanalysis of the Energy Efficient Stream Ciphers SSC2."

The SSC2 is a fast software stream cipher designed for wireless handsets with limited computational capabilities. It is the only one stream cipher which is special designed aim to energy efficient cryptography for wireless sensor networks in recent years open literatures. In this paper, the improved Guess-and-Determine attacks on both LFSR and lagged-Fibonacci half-ciphers of the SSC2 stream cipher are proposed. And some open problems about designing energy efficient stream cipher are discussed.

2.10pm
~
4.10pm

Lee, Suk-Bok, & Yoon-Hwa Choi. "ARMS: An Authenticated Routing Message in Sensor Networks."

In wireless sensor networks, a sensor node broadcasts its data (such as routing information, beacon messages or meta-data) to all its neighbors, which is called local broadcast. A general case for a sensor node to use a local broadcast is to advertise its routing information. Considering that sensor networks are vulnerable to a variety of attacks and current routing protocols are insecure, a sensor node's broadcast message should be authenticated by all its neighbors. Unfortunately, the previous work on broadcast authentication in sensor networks mainly concentrates on broadcast messages from a base station which has greater capabilities, not from a sensor node. Those schemes' properties are not appropriate for broadcast authentication of sensor node's routing messages. In this paper, we present ARMS, a protocol for broadcast authentication of sensor node's routing messages. It requires only a small memory space, authenticates routing messages without delay (thus, no buffering is needed), needs no time synchronization among sensor nodes, and mitigates the effect of packet loss. These ARMS' properties are suitable for a sensor node to broadcast an authenticated routing message.

Qiu, Ying, Jianying Zhou, & Robert Deng. "Security Analysis and Improvement of Return Routability Protocol."

Mobile communication plays a more and more important role in computer networks. How to authenticate a new connecting address belonging to a said mobile node is one of the key issues in mobile networks. This paper analyzes the Return Routability (RR) protocol and proposes an improved security solution for the RR protocol without changing its architecture. With the improvement, three types of redirect attacks can be prevented.

Gligor, Peralta, Krankis, Zheng, Burmester. Panel: "Authentication in Constrained Environments."

Designed by Jonathan C. Nilson. Published by Florida State University SAIT. Please see our website at http://www.sait.fsu.edu/madnes/ for more information.