[1] AirTight Networks, Inc. http://www.airtightnetworks.net. [bib]

[2] BelAir Networks, Inc. http://belairnetworks.com. [bib]

[3] Cranite Systems, Inc. http://cranite.com/. [bib]

[4] Fortress Technologies, Inc. http://www.fortresstech.com. [bib]

[5] MeshDynamics, Inc. http://www.meshdynamics.com. [bib]

[6] MeshNetworks, Inc. http://meshnetworks.com/. [bib]

[7] Nova Engineering, Inc. http://www.novaroam.com. [bib]

[8] Trapeze Networks, Inc. http://www.trapezenetworks.com. [bib]

[9] Tropos Networks, Inc. http://www.tropos.com/. [bib]

[10] A. AA-2004.02. Denial of service vulnerability in IEEE 802.11 wireless devices, May 13 2003. [bib | http]

[11] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *Network and Distributed System Security Symposium*, 2002. [bib | .html]

> In this paper we address the problem of secure communication and authentication in ad-hoc wireless networks. This is a difficult problem, as it involves bootstrapping trust between strangers. We present a user-friendly solution, which provides secure authentication using almost any established public-key-based key exchange protocol, as well as inexpensive hash-based alternatives. In our approach, devices exchange a limited amount of public information over a privileged side channel, which will then allow them to complete an authenticated key exchange protocol over the wireless link. Our solution does not require a public key infrastructure, is secure against passive attacks on the privileged side channel and all attacks on the wireless link, and directly captures users' intuitions that they want to talk to a particular previously unknown device in their physical proximity. We have implemented our system in Java for a variety of different devices, communication media, and key exchange protocols.

[12] S. Buchegger and J.-Y. L. Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In *Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing*, pages 403-410. IEEE Computer Society, January 2002. [bib | .html]

> Nodes in mobile ad hoc networks do not rely on a central infrastructure but relay packets originated by other nodes. Mobile ad hoc networks can work properly only if the participating nodes cooperate in routing and forwarding. For individual nodes it might be advantageous not to collaborate, though. The new routing protocol extensions presented in this paper make it possible to detect and isolate misbehaving nodes, thus making it unattractive to deny cooperation. In the presented scheme, trust relationships and routing decisions are made based on experienced, observed, or reported routing and forwarding behavior of other nodes. A hybrid scheme of selective altruism and utilitarianism is presented to strengthen mobile ad hoc network protocols in their resistance to security attacks, while aiming at keeping network throughput, or goodput, high. This paper focuses particularly on the network layer, using the Dynamic Source Routing (DSR) protocol as an example.

[13] S. Buchegger and J. Y. Le Boudec. Cooperative routing in mobile ad-hoc networks: Current efforts against malice and selfishness. In *Proceedings of Mobile Internet Workshop. Informatik 2002.*, October 2002. [bib | http]

> In mobile ad-hoc networks, nodes do not rely on any routing infrastructure but relay packets for each other. Thus communication in mobile ad-hoc networks functions properly only if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate, for example to save power or to launch security attacks such as denial-of-service. In this paper, we give an overview of potential vulnerabilities and requirements of mobile ad-hoc networks, and of proposed prevention, detection and reaction mechanisms to thwart attacks.

[14] L. Buttyán and J.-P. Hubaux. Report on a working session on security in wireless ad hoc

networks. *Mobile Computing and Communications Review*, 6(4), November 2002. http://lcawww.epfl.ch/Publications/Buttyan/ButtyanH02mc2r.pdf. [bib | .pdf]

[15] S. Capkun, L. Buttyán, and J.-P. Hubaux. Mobility helps peer-to-peer security. *To appear in IEEE Transactions on Mobile Computing*, 2005. http://icwww.epfl.ch/publications/documents/IC_TECH_REPORT_200381.pdf. [bib | .pdf]

> We propose a straightforward technique to provide peer-to-peer security in mobile networks. We show that far from being a hurdle, mobility can be exploited to set up security associations among users. We leverage on the temporary vicinity of users, during which appropriate cryptographic protocols are run. We illustrate the operation of the solution in two scenarios, both in the framework of mobile ad hoc networks. In the first scenario, we consider fully self-organized security: users authenticate each other by visual contact and by the activation of an appropriate secure side channel of their personal device; we show that the process can be fuelled by taking advantage of trusted acquaintances (the “friends” mechanism). In the second scenario, we assume the presence of an off-line certification authority and we show how mobility helps to solve the security-routing interdependency cycle; in this case, the security protocol runs over one-hop radio links. We then show that the proposed solution is generic: it can be deployed on any mobile network and it can be implemented either with symmetric or with asymmetric cryptography. We provide a detailed performance analysis by studying the behavior of the solution on various mobility models.

[16] M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Marti-Oliet, J. Meseguer, and C. Talcott. Maude 2.0 manual, 2003. http://maude.csl.sri.com/. [bib]

[17] M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, and C. L. Talcott. The Maude 2.0 system. In R. Nieuwenhuis, editor, *Proceedings of the 13th International Conference on Rewriting Techniques and Applications (RTA)*, volume 2706 of *Lecture Notes in Computer Science*, pages 76-87. Springer-Verlag, 2003. [bib | http]

[18] Cranite. Best practices: Wireless LAN design, implementation and management, Sep 2003. http://www.cranite.com/pdf/whitepapers/cranite-best-practices.pdf. [bib | .pdf]

[19] D. L. Dill. The murφ verification system. In *Proceedings of the Eighth International Conference on Computer Aided Verification CAV*, volume 1102, pages 390-393. Springer Verlag, July 1996. [bib | .html]

[20] Fortress. Public safety: Wireless-enabled patrol cars. Technical report, Fortress Technologies, Inc., White Paper, 2004. http://www.fortresstech.com/pdf/Public_Safety_Syracuse_Police.pdf. [bib | .pdf]

[21] C. He and J. C. Mitchell. Analysis of the 802.11i 4-way handshake. In *Proceedings of the 2004 ACM workshop on Wireless Security*, pages 43-50. ACM Press, 2004. [bib | DOI]

[22] 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*, Feb 2005. [bib]

[23] J. P. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, October 2001. [bib | http]

> So far, research on mobile ad hoc networks has been focused primarily on routing issues. Security, on the other hand, has been given a lower priority. This paper provides an overview of security problems for mobile ad hoc networks, distinguishing the threats on basic mechanisms and on security mechanisms. It then describes our solution to protect the security mechanisms. The original features of this solution include that (i) it is fully decentralized and (ii) all nodes are assigned equivalent roles.

[24] K. Jallad, J. Katz, and B. Schneier. Implementation of chosen-ciphertext attacks against pgp and gnupg. In *Proceedings of Information Security Conference*, 2002. [bib | .html]

> We recently noted that PGP and other e-mail encryption protocols are, in theory, highly vulnerable to chosen-ciphertext attacks in which the recipient of the e-mail acts as an unwitting “decryption oracle.” We argued further that such attacks are quite feasible and therefore represent a serious concern. Here, we investigate these claims in more detail by attempting to implement the suggested attacks. On one

hand, we are able to successfully implement the described attacks against PGP and GnuPG (two widely-used software packages) in a number of different settings. On the other hand, we show that the attacks largely fail when data is compressed before encryption.

Interestingly,the attacks are unsuccessful for largely fortuitous reasons; resistance to these attacks does not seem due to any conscious effort made to prevent them. Based on our work, we discuss those instances in which chosen-ciphertext attacks do indeed represent an important threat and hence must be taken into account in order to maintain confidentiality. We also recommend changes in the OpenPGP standard to reduce the effectiveness of our attacks in these settings.

[25] P. Lamsal. Survey of IETF security internet drafts, 2001. [bib | .pdf]

This document is a survey of the security related Internet drafts published by IETF. The Internet drafts presented here belong to different working groups of the security area of IETF. Important drafts from most of the working groups are described here.

[26] P. Lamsal. Survey of IETF security RFCs, 2001. [bib | .pdf]

This document is a survey of the security related standards or specifications published by IETF. The RFCs presented here belong to different working groups of the security area of IETF. Only half of the working groups have published RFCs and work is in progress in the remaining working groups. The main RFCs belonging to each of the working groups are described.

[27] P. Lamsal. Understanding trust and security, 2001. [bib | .html | .pdf]

This article is a literature survey on trust theory, the relationship between trust and security and distribution of trust in networks, especially in distributed and open networks. The article is divided into three sections: trust theory, security principles and trust distribution. The trust theory section looks at the theoretical aspects of trust and shows some of the methods researchers use to quantify trust. The security theory section explains the fundamentals of security and tries to establish a relationship between security and trust. This section also attempts to highlight the significance of trust in distributed network security. The final section considers ad hoc networks as one of the latest paradigms in wireless networking and looks at some proposals and initiatives aimed at establishing trust distribution in ad hoc networks.

[28] H. Luo, P. Zefros, J. Kong, S. Lu, and L. Zhang. Self-securing ad hoc wireless networks. In *Seventh IEEE Symposium on Computers and Communications (ISCC '02)*, 2002. [bib | .html]

Mobile ad hoc networking offers convenient infrastructure-free communication over the shared wire-less channel. However, the nature of ad hoc networks makes them vulnerable to security attacks. Exam-ples of such attacks include passive eavesdropping over the wireless channel, denial of service attacks by malicious nodes as well as attacks from compromised nodes or stolen devices. Unlike their wired counterpart, infrastructureless ad hoc networks do not have a clear line of defense, and every node must be prepared for encounters with an adversary. Therefore, a centralized or hierarchical network security solution does not work well.

This work provides scalable, distributed authentication services in ad hoc networks. Our design takes a self-securing approach, in which multiple nodes (say, k) collaboratively provide authentication services for any node in the network. This paper follows the design guidelines of [7] and makes several new contributions. We first formalize a localized trust model that lays the foundation for the design, and then expand the adversary model that the system should handle. We further propose refined localized certification services, and develop a new scalable solution of share updates to resist more powerful adversaries. Finally, the new solution is evaluated through simulations.

[29] C. Meadows. Formal methods for cryptographic protocol analysis: emerging issues and trends. *IEEE Journal on Selected Areas in Communications*, 21(1):44-54, January 2003. [bib | .html]

[30] MeshNetworks. Security issues & solutions in mobile ad hoc networks. Technical report, MeshNetworks, Inc., White Paper, Maitland, Florida, 2003. http://meshnetworks.com/pdf/wp_security_issues.pdf. [bib | .pdf]

[31] A. Mishra and W. A. Arbaugh. An initial security analysis of the IEEE 802.1X standard. Technical Report CS-TR-4328, University of Maryland, 2002. [bib]

The current IEEE 802.11 standard is known to lack any viable security mechanism. However, the IEEE has proposed a long term security architecture for 802.11 which they call the Robust Security Network (RSN). RSN utilizes the recent IEEE 802.1X standard as a basis for access control, authentication, and key management. In this paper, we present two security problems (session hijacking, and the establishment of a man-in-the-middle) we have identified and tested operationally. The existence of these flaws highlight several basic design flaws within 802.1X and its combination with 802.11. As a result, we conclude that the current combination of the IEEE 802.1X and 802.11 standards does not provide a sufficient level of security, nor will it ever without significant changes.

[32] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In *Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, pages 193-204, 2002. [bib]

The emergence of the Mobile Ad Hoc Networking (MANET) technology advocates self-organized wireless interconnection of communication devices that would either extend or operate in concert with the wired networking infrastructure or, possibly, evolve to autonomous networks. In either case, the proliferation of MANET-based applications depends on a multitude of factors, with trustworthiness being one of the primary challenges to be met. Despite the existence of well-known security mechanisms, additional vulnerabilities and features pertinent to this new networking paradigm might render such traditional solutions inapplicable. In particular, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. In particular, in MANET, any node may compromise the routing protocol functionality by disrupting the route discovery process. In this paper, we present a route discovery protocol that mitigates the detrimental effects of such malicious behavior, as to provide correct connectivity information. Our protocol guarantees that fabricated, compromised, or replayed route replies would either be rejected or never reach back the querying node. Furthermore, the protocol responsiveness is safeguarded under different types of attacks that exploit the routing protocol itself. The sole requirement of the proposed scheme is the existence of a security association between the node initiating the query and the sought destination. Specifically, no assumption is made regarding the intermediate nodes, which may exhibit arbitrary and malicious behavior. The scheme is robust in the presence of a number of non-colluding nodes, and provides accurate routing information in a timely manner.

[33] J. Schneider, G. Kortuem, J. Jager, S. Fickas, and Z. Segall. Disseminating trust information in wearable communities. In *2nd International Symposium on Handheld and Ubitquitous Computing (HUC2K)*, 2000. [bib | .html]

This paper describes a framework for managing and distributing trust information in a community of mobile and wearable computer users. Trust information in the form of reputations are used to aid users during their social interactions with the rest of the community.

[34] Trapeze. The illusion of security: Using IPsec VPNs to secure the air. Technical report, Trapeze Networks, Inc., White Paper. http://www.trapezenetworks.com/technology/whitepapers/illusionofsecurity/illusionofsecurity.pdf. [bib | .pdf]

[35] Tropos. Multi-layered security framework for metro-scale Wi-Fi networks. Technical report, Tropos Networks, Inc., White Paper, 2004. http://www.tropos.com/pdf/Tropos_Security_WP.pdf. [bib | .pdf]

[36] A. Vanhala. Security in ad-hoc networks. Research seminar on Security in Distributed Systems. Department of Computing Science, University of Helsinki., 2000. [bib | .html]

A short-range wireless channel has security problems that differ from those of more conventional networks. This paper presents first the general features of ad-hoc networks. Characteristic security issues in ad-hoc networks will be enlightened next. Finally, an example of a short-range wireless network will be presented. The Bluetooth standard is described shortly as well as the found

weaknesses in its security.

[37] C. D. J. Welch and M. S. D. Lathrop. A survey of 802.11a wireless security threats and security mechanisms. Technical Report ITOC-TR-2003-101, Department of Electrical Engineering and Computer Science, United States Military Academy at West Point, West Point, New York, 2003. http://www.itoc.usma.edu/Documents/ITOC_TR-2003-101_(G6).pdf. [bib | .pdf]

[38] L. Zhou and Z. J. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24-30, 1999. [bib | .html]

Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any xed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, we take advantage of the inherent redundancy in ad hoc networks | multiple routes between nodes | to defend routing against denial of service attacks. We also use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of our security framework.
