

Enabling Secure and Spontaneous Communication between Mobile Devices using Common Radio Environment

Alex Varshavsky Anthony LaMarca Eyal de Lara
University of Toronto Intel Research Seattle University of Toronto
walex@cs.toronto.edu anthony.lamarca@intel.com delara@cs.toronto.edu

Abstract

With the proliferation of mobile devices, spontaneous interactions between co-located devices that do not know each other a priori will become commonplace. Securing these interactions against eavesdropping and man-in-the-middle attacks is an important and challenging task. In this paper, we postulate that mobile devices that are positioned in close proximity may be able to derive a shared secret to secure their communication by monitoring fluctuations in the signal strength of existing ambient radio sources (GSM cell towers or WiFi access points) in their common environment. We explore the feasibility of deriving location-based secrets and describe two approaches for how such a secret could be used to secure spontaneous communication. Deriving location-based secrets is a hard problem because while the radio environment perceived by various devices in close proximity is similar, it is not identical.

I. INTRODUCTION

The number of mobile devices worldwide is growing rapidly. The percentage of households that own at least one mobile phone has reached more than 90% in South Korea, Japan and urban China, 80% in Western Europe, 75% in the United States and 60% in Canada [1]. Another survey revealed that 52% of American adults keep their cell phone turned on all the time while 40% of those between the ages of 18 and 29 say that they are increasingly likely to drop their landline once and for all [2].

We envision that with the increased adoption of mobile devices, spontaneous interactions between co-located devices that do not know each other a priori will become commonplace. For example, patrons at a bar, guests at a party or conference participants may want to exchange private contact information, or teenagers who run into each other at a mall may want to play a game on their smart phones. Moreover, people are likely to interact with stationary radio equipped devices as well.

For example, consumers may want to pay for groceries at a store or tickets at a train station using their mobile phones, or a user may want to take advantage of resources available in the environment by pairing her mobile phone to a public full-sized display and keyboard [3].

We argue that an important condition for the widespread proliferation of spontaneous interactions is securing the interactions against eavesdropping and man-in-the-middle attacks. Obviously, nobody would want her private contact or banking information to be overheard and tampered with by a malicious third party. Unfortunately, most existing techniques for establishing secure channel between devices require either significant user attention (e.g., requiring the user to type in passwords [4]) or specialized hardware present on the mobile devices (e.g., ultrasonic receivers [5]).

We consider that two devices may interact securely with each other if they share a secret key that can be used to encrypt their communication. We further refer to the problem of securing spontaneous communication between co-located mobile devices as *secure pairing*.

In this paper, we postulate that it may be possible to securely pair devices in close proximity (a few centimeters apart) by deriving a shared secret from characteristics of their common radio environment. We take advantage of three observations: First, many mobile devices come equipped with radios that can sense their immediate radio environment. Second, devices in close proximity that simultaneously monitor a common set of ambient radio sources (e.g., WiFi access points or GSM base stations) perceive a similar radio channel. Third, due to environmental factors the radio channel varies unpredictably over time. For

example, signal strength from a given GSM base station as measured at a fixed location fluctuates from one moment to the next. Together, these observations imply that it may be possible for devices in close proximity to derive a common radio profile that is specific to a particular location and time. We hypothesize that this common radio profile can form the basis for a shared secret that can be used to securely pair devices in close proximity.

In the rest of this paper, we explore the feasibility of securely pairing devices based on characteristics of their common radio environment. Section II formalizes the problem of securely pairing devices in close proximity, and outlines two ways in which location-based secrets could be used to securely pair devices. Section III presents evidence that suggests that devices in close proximity may be able to derive a shared time and location specific secret by monitoring their radio environment. Section IV discusses challenges for deriving time and location specific secrets. The design of practical algorithms that derive a shared secret based observations of the radio environment is the subject of our future work. Finally, sections V and VI discuss related work, and present our conclusions.

II. SECURE PAIRING OF CO-LOCATED DEVICES

We define the problem of secure pairing of co-located devices as follows. Two co-located devices, A and B, want to establish a secure communication channel with each other in the presence of other malicious devices located nearby that may try to impersonate either A or B. Although A and B do not know each other a priori, they know that they are co-located. The assumption is that A and B both have compatible radios (e.g., WiFi or GSM) that they use for communication with each other and for deriving a shared secret based on monitoring their common radio environment. We assume no other hardware such as infrared ports or accelerometers is present on a device.

Next, we outline two ways in which location-based secrets could be used to securely pair devices. The main idea of both methods is that it is hard to guess fluctuations in the radio environment at a specific location and at a specific time without being physically present at that location and at that time.

Location-Based Authentication Token

Single-use location-based authentication tokens derived from the common wireless environment could be used to augment traditional key exchange techniques, such as Diffie-Hellman [6], with location-based key authentication. The authentication token, in essence, removes the need to access the public-key infrastructure (PKI) to do key validation. Instead, a token provides proof that a key was obtained from a device that is physically present in the same location. Because the authentication token is used only to validate the keys being exchanged, but not as the basis for encryption, the token does not have to remain secret once the key exchange takes place. The implication is that the token can be small as the system only needs to make sure that the probability of guessing the token at communication establishing time is small (e.g., 1 in a million).

Location-Based Encryption Keys

Unfortunately, performing Diffie-Hellman exchange on CPU handicapped devices may be infeasible. Toward this end, we conjecture that it may be possible to derive a shared key from the shared radio environment directly and thus eliminate the need for the expensive Diffie-Hellman exchange.

III. REQUIREMENTS ON RADIO ENVIRONMENT

In this section, we present experimental data that suggests that devices in close proximity may be able to derive a shared secret by monitoring their radio environment. Secure pairing imposes three requirements on the characteristics of the radio environment as perceived by the co-located devices. First, the signal at any specific location should fluctuate unpredictably over time. Otherwise, an attacker who collected radio measurements some time ago at the same location where the current pairing is taking place may

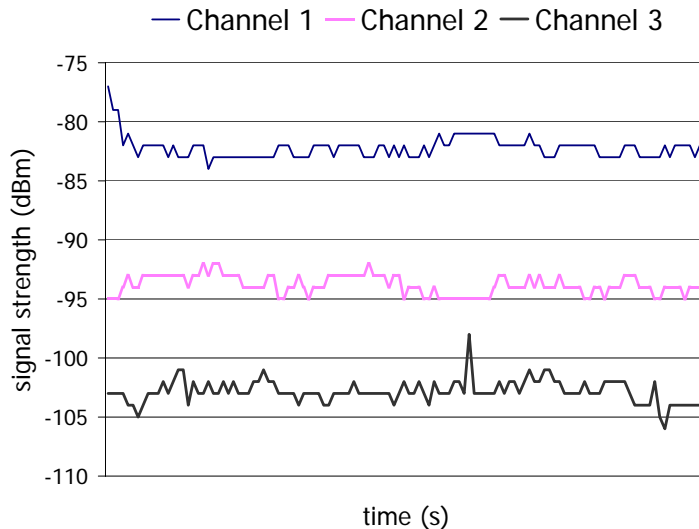


Fig. 1. The variation of signal strength over time on 3 GSM channel at the same location over 10 minutes

succeed in impersonating one of the target devices. Second, the signal at two different locations some distance apart should fluctuate differently over the same period of time. If not, an attacker located some distance away from the location where the current pairing is taking place may succeed in impersonating one of the target devices. Finally, in order for the two devices in close proximity to derive a shared secret, from which a location-based token or key is synthesized, the radio environment as perceived by the two co-located devices should exhibit at least some similarity.

Since most existing mobile devices are equipped with a cellular radio, we conducted a set of preliminary experiments where we tested whether GSM radio environment meets the above-mentioned requirements. First, we collected a series of GSM measurements at a single location using a Sony Ericsson GM29 GSM modem. We polled the GSM modem every 5 seconds, as we found experimentally that this interval is sufficient for the GSM modems to update their internal view of the radio environment. Figure 1 presents the variation of GSM signal strength over 10 minutes on three different GSM channels at a single location. The figure shows that GSM signals indeed fluctuate unpredictably on a small scale over time, thus preventing an attacker from gaining the system by fingerprinting the location, meeting the first of the above requirements.

Next, we positioned antennas of two “legitimate” GSM modems, m1 and m2, in close proximity to each other and an antenna of a third “attacker” GSM modem 2 meters away and collected a series of GSM measurements over a 5 minute period. All three GSM modems observed signals from the same 14 GSM channels. The goal of the experiment was to investigate the similarity of the signal strength fluctuations between the three possible pairs of modems. To understand the similarity, we calculated Pearson correlation coefficients between readings of the three pairs of modems on each of the 14 GSM channels. The Pearson correlation coefficient captures the tendency of the two streams of readings to increase or decrease in value simultaneously. The Pearson correlation coefficient value of 1 means a perfect correlation, the value of 0 means no correlation and the value of -1 means perfect negative correlation.

Table I presents the Pearson correlation coefficients between each pair of modems on each of the GSM channels and Figure 2(a) shows the signal strength variation over the 5 minute period on the 6th GSM channel. The signals in the figure were shifted on the y-axis for better presentation, but left to scale. The results suggest that while the measurements of m1 and m2 show some correlation, it will be hard to differentiate between fluctuations of the legitimate modem and an attacker who is located 2 meters away. We are planning to experiment with an attacker who is positioned farther away in the near future.

14 GSM Channels														
m1 - m2	0.54	0.16	-0.63	-0.81	0.01	0.04	-0.14	0.23	0.34	0.31	0.58	0.46	0.02	0.32
m1 - attacker	-0.12	0.17	0.67	0.40	0.05	-0.34	-0.04	-0.05	0.47	0.34	0.36	0.10	0.03	0.32
m2 - attacker	0.02	0.06	-0.48	-0.36	-0.31	0.17	0.17	0.12	0.21	0.03	0.32	0.02	0.02	0.19

TABLE I

[UNOBSTRUCTED ANTENNAS] PEARSON CORRELATION COEFFICIENTS ON 14 GSM CHANNELS

14 GSM Channels														
m1 - m2	0.68	0.67	0.53	0.48	0.59	0.79	0.66	0.68	0.32	0.73	0.75	0.64	0.64	0.80
m1 - attacker	0.08	-0.15	-0.06	0.05	0.26	-0.02	0.01	0.09	0.06	0.03	-0.17	-0.16	0.06	0.40
m2 - attacker	0	0	0.05	0.29	0.38	-0.01	-0.18	0.20	0.22	0.11	-0.20	-0.41	0.06	0.47

TABLE II

[HAND OBSTRUCTED ANTENNAS] PEARSON CORRELATION COEFFICIENTS ON 14 GSM CHANNELS

We repeated the experiment again, but this time one of the authors repeatedly covered the antennas of m1 and m2 with his hand. Table II presents the Pearson correlation coefficients between each pair of modems on each of the GSM channels and Figure 2(b) shows the signal strength variation over the 5 minute period on the 6th GSM channel for the hand obstructed experiment. The results show that covering the antennas resulted in a much better correlation between signals of co-located devices and low correlation between signals of the legitimate devices and the attacker. Thus we conclude that there is enough similarity between the signals of the legitimate modems to enable them to synthesize a shared secret (condition 3 above), and that an attacker positioned even just 2 meters away will not be able to guess the secret (condition 2 above).

We argue that repeatedly covering the antenna (e.g., by waiving the hand in front of it) will not impose significant burden on the user, as it does not require the user to physically move the antenna around (i.e., the user will not have to dance with the vending machine in order to securely pay for his cola). Although not requiring the user to perform any actions for secure pairing is our eventual goal, some gesticulation may be justified if it brings the user extra security.

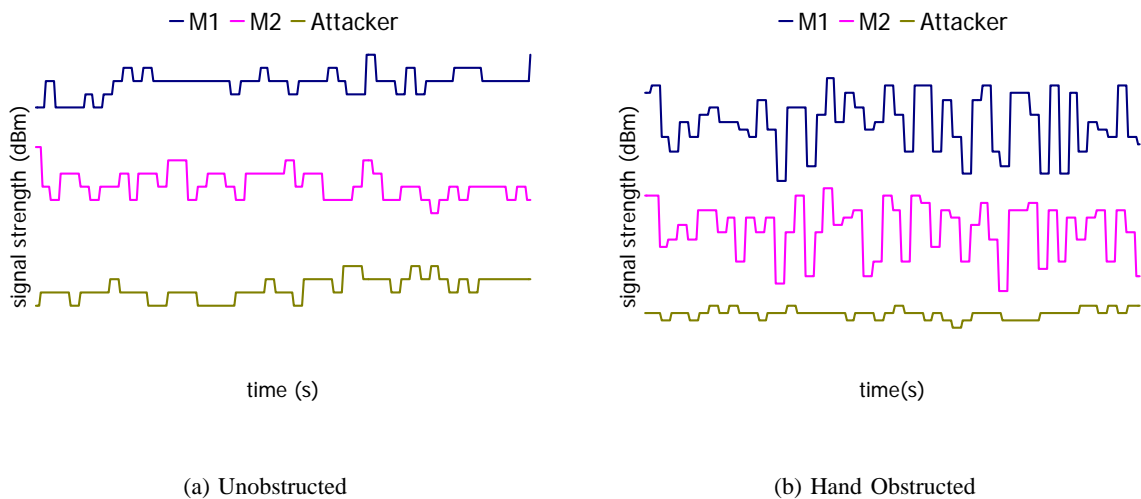


Fig. 2. The variation of signal strength over 5 minutes from three GSM modems in unobstructed and hand obstructed experiments. M1 and M2 are positioned closely together, while the attacker modem is 2 meters away.

IV. CHALLENGES

Developing an algorithm that creates a location-based authentication token or encryption key from two streams of radio measurements is an open research problem. This problem is challenging because although the shared radio environment as perceived by two co-located devices is similar, it is not identical. The algorithm that derives the location-based authentication token or encryption key should satisfy four requirements. First, the algorithm should be tolerable to a degree of non-similarity in the perceived radio environment, but at the same time, make it hard for the attacker to guess the key or the token directly. Second, the algorithm should work well, independent of the antenna configuration of the target devices, because co-located devices will not necessarily be from the same manufacturer or module. Third, it should not require a large number of measurements because users are unlikely to use the scheme if it takes a long time to perform the pairing. Finally, it should work well even if the radio measurements were collected at slightly different moments because the clocks on the two co-located devices may not be precisely synchronized.

We conjecture that the following common features of the streams of radio measurements can be used by the algorithm: (a) the rate of signal fluctuations; (b) the Fourier transform of the signal (c) the amplitude of signal fluctuations; (d) the direction of the signal strength change; (e) the quantized signal strength values over time; (f) the radio channels that appear in the radio measurement; (g) difference in signal strength across channels; and (h) correlation between changes across different channels as opposed to within a channel. We are currently experimenting with all these techniques and are hoping to develop an algorithm for secure pairing of co-located devices in the near future.

V. RELATED WORK

In Bluetooth, users pair devices by entering a secret PIN number. While the PIN provides for device authentication it requires user involvement. Moreover, Bluetooth pairing has been shown to be susceptible to eavesdroppers equipped with directional antennas that allow them to breach the security of the system from more than a mile away [7], [4].

Several research projects have suggested the use of physically constrained channels as a means of establishing secure association between devices in close proximity. Some examples include the use of a direct electric contact [8], infrared beacons [9], [10], ultrasound [5], and laser beams [11]. Unfortunately, physically constrained channels often require extra special hardware (e.g., an extra cable that users have to haul with them), and are susceptible to attacks by sensitive receivers that can detect dim signal refractions and reflections [7], [4].

In Shake Them Up! [12], two devices establish a shared secret over an anonymous broadcast channel by taking turns in transmitting parts of the key. To prevent attackers from exploiting power analysis to break the channel anonymity by correlating wireless transmissions to specific devices, users have to shake their devices to randomize the reception power of their packets by a potential eavesdropper. Unfortunately, this approach is vulnerable to attack by a determined eavesdropper who can exploit small differences in the baseband frequencies of the two radio sources, which result from differences in their crystal clock oscillators, to differentiate between packets sent by the two transmitters. Smart-It [13] used common readings from accelerometers to establish an association between devices by shaking them together. This solution, however, also requires devices to be augmented with additional hardware. LoKey [14] uses SMS messages to authenticate key exchanged over the Internet. This approach, however, may incur significant monetary cost and delay.

In contrast, we propose to securely pair wireless devices by using their common radio environment as proof of close proximity – devices that see the same radio environment are probably close by. Our approach takes advantage of the existing radio interfaces already present on many mobile devices (e.g., WiFi, GSM), and does not require any additional hardware. Finally, because the shared secret used to secure communication is attained by listening to the common radio environment, as opposed to transmitting, our approach is not susceptible to eavesdropping attacks.

VI. CONCLUSIONS

In this paper, we presented an open research problem of the secure pairing of co-located devices using their common radio environment. We argued that mobile devices that are positioned in close proximity may be able to derive a shared secret to secure their communication by monitoring fluctuations in the signal strength of existing ambient radio sources (GSM cell towers or WiFi access points) in their common environment.

We explored the feasibility of deriving location-based secrets and described two approaches for how such a secret could be used to secure spontaneous communication. Both approaches rely on the assumption that it is hard to guess fluctuations in the radio environment at a specific location and at a specific time without being physically present at that location and at that time. The first approach suggests deriving a single-use location-based authentication token from the common wireless environment and using it to augment traditional key exchange techniques, such as Diffie-Hellman [6], with location-based key authentication. The second approach, suggests deriving a shared secret key directly from the shared radio environment, thus eliminating the need for the expensive Diffie-Hellman exchange.

Finally, we outlined challenges for securely pairing devices using their common radio environment and presented a list of signal features that may be used to solve the problem. We are currently developing algorithms for the secure pairing of co-located devices and hope to present our findings to the research community in the near future.

REFERENCES

- [1] "USA Today, http://www.usatoday.com/tech/news/2006-04-19-mobile-use-up_x.htm," .
- [2] "Technology News <http://www.technewsworld.com/story/49849.html>," .
- [3] John J. Barton, Shumin Zhai, and Steven Cousins, "Mobile phones will become the primary personal computing devices," in *IEEE Workshop on Mobile Computing Systems and Applications*, April 2006.
- [4] Yaniv Shaked and Avishai Wool, "Cracking the bluetooth pin," in *Proc. of Mobisys*, 2005.
- [5] T. Kindberg and K. Zhang, "Validating and securing spontaneous associations between wireless devices," in *Proc. of Information Security Conference*, 2003.
- [6] W. DIFFIE and M. HELLMAN, "New directions in cryptography," *IEEE Transactions on Information Theory*, pp. 644–654, 1976.
- [7] H. Cheung, "How to: Building a bluesniper rifle - part 1, http://www.tomsnetworking.com/2005/03/08/how_to_bluesniper_pt1," March 2005.
- [8] F. Stajano and R. J. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," in *Proc 7th Security Protocols Workshop*, 1999.
- [9] D. Balfanz, D. Smetters, P. Stewart, and H.C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks," in *Proc. Network and Distributed Systems Security Symposium*, 2002.
- [10] Diana Smetters, Dirk Balfanz, Glenn Durfee, Trevor Smith, and KyungHee Lee, "Instant matchmaking: Simple, secure virtual extensions to ubiquitous computing environments," in *Proc. 8th International Conference on Ubiquitous Computing*, 2006.
- [11] T. Kindberg and K. Zhang, "Secure spontaneous device association," in *5th International Conference on Ubiquitous Computing*, 2003.
- [12] Claude Castelluccia and Pars Mutaf, "Shake them up!: a movement-based pairing protocol for cpu-constrained devices," in *Proc. of MobiSys*, 2005, pp. 51–64.
- [13] Lars Erik Holmquist, Friedemann Mattern, Bernt Schiele, Petteri Alahuhta, Michael Beigl, and Hans-W. Gellersen, "Smart-its friends: A technique for users to easily establish connections between smart artefacts," in *Proc. of UbiComp*, 2001.
- [14] Anthony J. Nicholson, Ian E. Smith, Jeff Hughes, and Brian D. Noble, "Lokey: Leveraging the sms network in decentralized, end-to-end trust establishment," in *Proc. of Pervasive*, 2006.