Simple and Effective Defense Against Evil Twin Access Points

Volker Roth
FX Palo Alto Laboratory

Wolfgang Polak
FX Palo Alto Laboratory

Eleanor Rieffel
FX Palo Alto Laboratory

Thea Turner
FX Palo Alto Laboratory

ABSTRACT

Wireless networking is widespread in public places such as cafés. Unsuspecting users may become victims of attacks based on "evil twin" access points. These rogue access points are operated by criminals in an attempt to launch man-in-the-middle attacks. We present a simple protection mechanism against binding to an evil twin. The mechanism leverages short authentication string protocols for the exchange of cryptographic keys. The short string verification is performed by encoding the short strings as a sequence of colors, rendered sequentially by the user's device and by the designated access point of the café. The access point must have a light capable of showing two colors and must be mounted prominently in a position where users can have confidence in its authenticity. We conducted a usability study with patrons in several cafés and participants found our mechanism very usable.

Categories and Subject Descriptors

H.1.2 [**Models and Principles**]: User/Machine Systems—*Human factors, Human information processing*; H.5.2 [**Information Interfaces and Presentation**]: User Interfaces—*Interaction Styles, User-centered design*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Authentication, Unauthorized access*

General Terms

Experimentation, Measurement, Human Factors, Security

Keywords

Device Pairing, Evil Twin, Usable Security, Wireless Security

1. INTRODUCTION

As wireless technology proliferates there is a growing concern about fraud and phishing attacks based on so-called "evil twin" wireless access points [8, 18, 4, 30, 1]. The evil twin is deployed and controlled by a malicious adversary and mimics a genuine access point. Public places, like cafes or airport terminals, are particularly susceptible to this form of attack. Unsuspecting users who bind to the evil twin compromise their network communications: their login information and passwords can be stolen, or their browsers redirected to look-alike phishing websites and download pages containing malware.

The ease with which an evil twin can be set up has been demonstrated using, for example, *Airsnarf* [11]. Since evil twins provide gateway services and DNS settings to connecting clients, hackers gain full control over the clients' network communications. For instance, the evil twin may map the authentic domain name of a banking website to the IP number of a phishing website. This undermines a major trust indicator for the user: the URL displayed in the user's browser. Additional tools such as *Ettercap* [20] come with extensive support for *man-in-the-middle* attacks on unencrypted, and even encrypted, communications.

Detection is difficult for users because the access point to which a user's device binds does not identify itself in a fashion that can be verified reliably by the user. Without cables, an important implicit ingredient of traditional security policies is missing: the assurance that our device is connected to a specific physical *endpoint* [2]. Instead, wireless devices establish *virtual endpoints* through advertisement and discovery [23]. Our mechanism provides an alternative physical assurance for a user of wireless technology.

The evil twin problem is closely related to the general problem of pairing two wireless devices, which has attracted a significant amount of research. We compare our approach extensively with related work in §3. For brevity, we mention here merely that existing solutions are good choices in many cases, but have disadvantages or limitations in our motivating scenario.

Our aim was to design a mechanism to defeat evil twin attacks that would enable a user to easily verify the connection with little prior training or knowledge. Following [24], the mechanism must be "psychologically acceptable"; in other words, it should be easy to understand and use by people who access the Internet from public locations. Similarly, we wished to use a minimum of hardware so that our mechanism could be used even by small, inexpensive devices with limited display capabilities.

The simplest solution we have developed to date leverages existing key establishment protocols [32, 9, 33] based on *short authentication strings.* We require only that the wireless access point has a light capable of showing two colors, and that the device has at least one button in addition to such a display capability. Each short authentication string is converted into a color sequence composed of two different colors. Both the wireless access point and the user's device render the sequences one color at a time. The access point's light must be mounted where café patrons can see it and have confidence that it belongs to the café's authentic access point. When the user presses a designated button on her device, both lights show the next color in the sequence. The colors are shown for as long

WiSec'08, March 31–April 2, 2008, Alexandria, Virginia, USA.

as the button is held down, so patrons can see the colors as long as they need to effectively compare them. The user can choose how much of the sequence to compare depending on her desired level of security. Once the user has completed her comparisons, she indicates whether she accepts or declines the connection by means of a designated button or other means of input. A detailed description of the mechanism, and a discussion of its properties, is given in §2.

In order to verify our hypothesis that this mechanism would be easy to use, we built a simulator and conducted a user study with it in several cafés. In this fashion, we expected to recruit a representative sample of our target users. Furthermore, the setting was more realistic than a laboratory setting would have been. At the same time, we had to expect that participants were less attentive and subject to distractions such as environmental noise and moving patrons. Nevertheless, our study participants found our mechanism to be very usable. A detailed description of the study, its outcomes and our interpretation of results is given in §4.

2. PROTECTION MECHANISM

2.1 Threat Model and Assumptions

We assume that the attacker can operate a rogue access point that competes with the authentic access point of a location such as a café. The rogue access point may have the capability to mimic the authentic access point perfectly except for access to secret key material. However, the attacker shall not be able to subvert or replace the authentic access point. In particular, the attacker cannot manipulate the access point's light, which can be external to the access point, in any other way than by manipulating the communication channel. The attacker may operate the rogue access point in a concealed fashion. However, we assume that any rogue access point mounted in a prominent place, where patrons could mistake it for the authentic access point, will be discovered and removed by the café personnel. We do not consider denial of service attacks.

2.2 Design Considerations

Protection mechanisms must be designed not only with technical requirements and risks in mind, but also with consideration of how end-users interact with the mechanism. This design principle has been emphasized in the classic security literature, for instance by Saltzer and Schroeder in [24], who refer to it as *psychological acceptability.*

Concrete guidance as to how psychological acceptability can be achieved is given in the human computer interaction literature for instance by Shneiderman [27]. He highlights eight "golden rules" for interface design, of which two are particularly relevant for the class of mechanisms we address in this paper:

Internal locus of control: Operators should be given the feeling that they are in charge of the system and that the system responds to their actions.

Our mechanism responds to users' button presses by lighting up for as long as the button is depressed. The user also chooses how many comparisons to perform. Both of these features give the user direct control over the interaction. The user would have less control if the colors changed automatically. In another design, the user could observe the color displayed by the access point, and then enter it into her own device using two buttons. However, when a user enters information, the user is responding to the system, as opposed to the system responding to the user.

Reduction of short-term memory load: The displays should be kept simple and users' tasks should ideally not require memorization.

At any given time during the interaction, only two items must be retained and the operation to be performed by the user is a simple decision whether the two items are equal. Briefly, our mechanism incurs minimal load on short-term memory (see also §4) whereas these other mechanisms operate at what is considered maximum load [19, 34].

In those cases where the user's device is capable of graphical output and non-trivial input it may be sufficient to perform our mechanism only once and to cache the public key of the encountered access point. The *user* would then choose and associate a suitable identifier for that key on the device (note that the identifier is not supplied by the access point, which could be spoofed). The device can display the identifier whenever the associated key is encountered again, and thereby informs the user unambiguously to which network it is going to bind.

2.3 Short Authentication Strings

In our scenario, we cannot assume that the user's device and the wireless access point share a secret key or possess public key certificates signed by mutually trusted third parties. Instead, the devices exchange public keys over the insecure wireless channel, and use them to secure their communication. The user thwarts man-in-the-middle attacks by authenticating the exchanged keys over the low-bandwidth (authenticated) visual channel. This can be accomplished efficiently by "short authentication string" protocols as they have been described and proven secure e.g. in [32, 33, 14].

During the setup phase, the two devices commit to their public keys and nonces N_A and N_B. The nonces can be short, hence the name "short authentication strings." However, they should be longer than the maximal number of comparisons the user is willing to perform. If the protocol proceeds without interference then the sent and received nonces are identical i.e., $N_A = N'_A$ and $N_B = N'_B$. Under a man-in-the-middle attack by an evil twin, the protocol assures that with high probability $N_A \neq N'_A$ so $N_A \oplus N'_B \neq N'_A \oplus N_B$. The probability of such an occurrence is unconditional of the amount of computational power the adversary has [14]. The point of the verification is to distinguish these two cases.

Our work is concerned with a particular technique, suitable in the settings described earlier, for realizing the authenticated channel and performing the short string comparison. The authenticated channel is essentially made up of two channels; the user can physically observe lights on both devices, creating two authenticated channels from A and B to the user. We assume that the user controls device B. Instead of sending $N'_A \oplus N_B$ through one authenticated channel to A where it is compared with $N_A \oplus N'_B$, both devices display their respective values through their lights to the user who performs the comparison.

Instead of just showing the user two parallel sequences of colored lights, the user will be actively involved in controlling the comparison. The bit strings $N_A \oplus N'_B$ and $N'_A \oplus N_B$ define two sequences of colors that agree when there is no intruder. By pressing a button on device B, the user turns on the next color of the respective sequence in each device. As long as the user holds the button, the lights remain on, allowing to user to determine the time needed for comparison. Device B will relay the user's button push to device A through the open, high-speed channel. By interfering with this channel, an intruder will be able to suppress a click, alter the duration of the light, or create additional clicks. To ensure that these changes will be detected by the user we require that each light remains lit for a perceptible minimum time.

The user can choose the number of button clicks to use based on the required security. When the user is satisfied that there has been no intrusion, she will signal "accept" to device B, which completes the protocol.

In an environment where multiple users try to authenticate a shared device (e.g. a Wi-Fi access point), the shared device needs to sequentialize authentication requests. Based on our user study, the expected time for visual verification of short authentication strings will be less than 20 seconds. For most applications the frequency of authentication requests is not likely to create excessive waits.

3. RELATED WORK

The problem of pairing wireless devices has drawn significant attention by the research community. Several authors have published protocols whereby two devices establish authentic keys based on short authentication strings [32, 9, 33]. These protocols serve as a blueprint for the mechanisms under standardization for Bluetooth Simple Pairing, Wi-Fi Protected Setup, Wireless USB Association Models and HomePlugAV security modes (see [29, 31, 13] for comparative analysis and overviews). The practical security of these protocols is independent of the amount of precomputation [14] but depends on the length of the short strings the user compares or enters diligently. We leverage this category of protocols in our protection mechanism.

Several researchers have suggested alternative renderings that could be used in conjunction with hash verification [16] and short authentication strings, including human-readable words [12], flag-like symbols [7], and random art [21]. Renderings of this kind would be difficult for users to see, for example, across a room. Additionally, the access point would require a sufficiently large and complex display, which adds significantly to the cost of the access point. A single light, on the other hand, can be perceived easily and consistently at various distances.

Speech [10] or other audio renderings would likely annoy other patrons and might be difficult to hear if the environment is noisy due to music played by the café, loud conversations nearby, or outside vehicle traffic.

Security associations can also be formed by physical contact [6, 28, 3]. However, such mechanisms inconvenience patrons since they would have to leave their table to move close to the access point in order to complete the pairing. For the same reason, synchronous trigger events [22] would be undesirable.

Directed location-limited channels that can be decoded automatically may be more applicable. However, not all mechanisms proposed in the literature are suitable in our scenario. For instance, mechanisms based on camera recordings of detailed renderings [17, 26] would be affected by larger distances (and again require suitable rendering capabilities at the access point). Modulation can compensate for the larger distance by encoding complex information as a sequence of simpler signals rendered by displays as simple as a single LED [26]. However, the sensor that decodes the signals is typically affixed to the user's device and therefore the entire device would have to point towards the signal source. While this is easy with a mobile phone it is inconvenient with a laptop. Furthermore, longer distances and unpredictable environmental conditions may cause a high decoding error rate, whereas humans are significantly better at the task of locating and perceiving a light.

Undirected location-limited channels that operate at a sufficiently large distance would again be susceptible to man-in-the-middle attacks. Distance bounding protocols [5, 33, 25] provide limited assurance in this case since they are only effective against adversaries that are farther away from the user than the access point. However, in a café, the attacker may sit only one table away from the user.

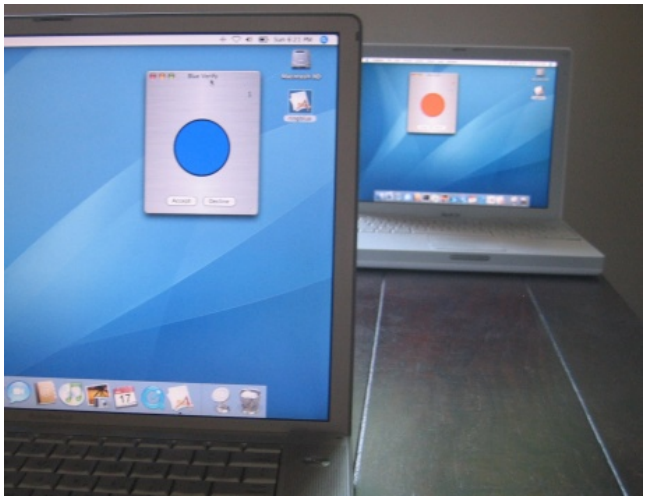


Figure 1: Shows the experimental setup used in the user study. The far laptop simulates the wireless access point. In this case, the color difference indicates an attack.

Our observations of environmental and application constraints suggest that our protection mechanism fills an important niche of practical relevance. It is surprising that, despite its simplicity, the combination of short authentication string protocols and color--coded binary comparison tasks has, to the best of our knowledge, not been suggested elsewhere. On the contrary, in their comparative study of Wi-Fi Protected Setup and Bluetooth Simple Pairing, Kuo et al. [13] argue that secure pairing is not possible in a usable fashion if the pairing devices only have an LED and a button. Our protection mechanism scores well along all compared dimensions (security, usability, cost of manufacture).

4. USER STUDY

4.1 Materials and Methods

We implemented a proof of concept prototype of our mechanism for our user study. The prototype simulated the session setup through a Bluetooth connection between two laptops. Each laptop showed a user interface with a colored circle as the light indicator. The circle was filled black if the light was off and filled blue or orange otherwise. The lights were operated by pressing and holding the 'A' button on the keyboard of the near laptop. Figure 1 shows a representative setup in which the colors displayed by both laptops differ and thereby indicate an attack.

We also prepared information material and questionnaires which were provided to the participants of our study. The material explained briefly the purpose and functioning of the mechanism. We also provided guidance in regard to what numbers of comparisons would yield a low, medium or high level of security (low: 5–6, medium: 9–10, high: 16–20). This guidance was not meant to be accurate nor authoritative but to establish a consistent reference point for all study participants.

The questionnaires were divided into a pre-condition background questionnaire and a post-condition feedback questionnaire. In the background questionnaire, we asked basic demographics.

The post-condition questionnaire included 11 statements with which subjects had to agree or disagree on a nine point Likert [15] scale. The statements are given in Fig. 3. Additionally, we asked four questions (see Fig. 4) how subjects perceived the lights, their

1. I have a strong background in computers.
2. I have been the victim of Internet fraud e.g., phishing.
3. I know someone who has been the victim of Internet fraud.
4. I believe that wireless Internet access in cafés is generally secure.

Figure 2: Questions used in the background questionnaire. Questions 2-3 required yes/no answers; the other questions used a nine point Likert scale.

security goals and their estimate of the average number of comparisons they had performed per session.

We randomly recruited 20 subjects in several cafés in Palo Alto and San Francisco during afternoon and evening hours. The experiments were conducted in the cafés where we recruited the subjects. In this way we expected to obtain a representative sample of our target users. Furthermore, the experiments took place in a realistic setting, which included occasionally bright sunlight and ambient noise. All subjects reported that they were not color-blind.

Of our 20 subjects, seven were male and younger than 40 years, seven were male and older than 40, and the remaining six female subjects were all younger than 40 years. We did not find females older than 40 years who were laptop users. We removed one subject from the dataset because he appeared to be unable to understand the task requirements. This left us with 19 usable datasets.

Each subject performed seven sessions with our mechanism. The first two sessions were used to explain the mechanism and to enable subjects to familiarize themselves with it. The subsequent five rounds counted for the study. The prototype was programmed to introduce color differences in odd rounds. A color difference would occur only after the first four comparisons with a probability of 0.2. In a realistic setting, the probability should be close to 0.5. By lowering the probability, we increased the likelihood of longer color sequences without a color difference. We were concerned that, otherwise, subjects would be conditioned to perform few comparisons. A side effect of this choice was that we observed fewer than the maximal number of sessions with color differences because some subjects would accept a session that was scheduled to have a color difference before the difference occurred.

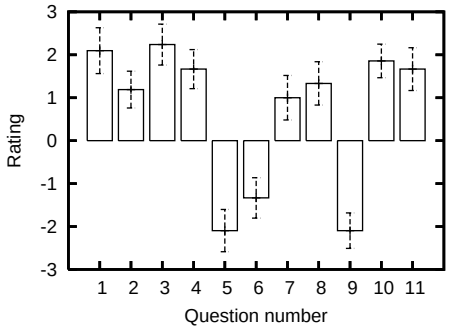
4.2 Results

Subjects

Our subjects were 20–60 years old with an average age of 35 years. The subjects agreed that they have a strong computer background ($\bar{x} = 2.37; se = 0.31$). Three subjects reported that they are victims of Internet fraud and seven reported that they know someone who is a victim. Seventeen subjects focused on either the far or the near light. Sixteen subjects perceived the two lights simultaneously and three reported that they looked back and forth. Ten subjects aimed for a low level of security, nine for a medium level and no subjects aimed for a high level.

Questionnaire

We analyzed the answers to our post-condition questionnaire and illustrate the results in Fig. 3. Subjects disagreed with the statements that our mechanism requires a lot of mental work, is tiring and takes too long to achieve the desired level of security. On the other hand, they were confident that they noticed all color differences. Furthermore, subjects found our mechanism easy to use and professional. These answers were correlated ($r = 0.78; t = 5.14; p < 0.001$), which appears to differ from what Uzun et al. found [31]. In their comparative study of three secure pairing methods, the method that was rated the least usable was rated the most professional, and vice versa. Subjects also agreed that securing their wireless connection was well worth the effort, and they also expressed a preference for our mechanism over having to enter a password or PIN. Some subjects mentioned that they liked the fact that they did not have to remember anything.



1. I am sure that I noticed all color differences.
2. I had fun using the mechanism.
3. The mechanism is very easy to use.
4. The mechanism is very professional.
5. The mechanism requires a lot of mental work.
6. I was getting tired using the mechanism.
7. I would like to use the mechanism every once in a while.
8. I would like to use the mechanism every time I come to the café.
9. It took too long to achieve the security I wanted.
10. Making my wireless connection secure was well worth the effort.
11. I would prefer the mechanism over entering a password or PIN.

Figure 3: Graphs the mean and standard error of subjects' answers to our post-condition questionnaire. Answers were given as agreement or disagreement with the statements above on a nine point Likert [15] scale.

1. On which light did you focus your gaze?
   The close light ☐ / the far light ☐ / between lights ☐
2. How did you perceive (attended to) the two lights?
   Simultaneously ☐ / I looked back and forth ☐
3. The level of security I tried to achieve was:
   Low ☐ / Medium ☐ / High ☐
4. On average, I believe that I performed ____ clicks per session.

Figure 4: Additional questions we asked on our post-condition questionnaire.

Measurements

Two subjects only performed four sessions. One subject accidentally double-clicked the accept button and the second subject omitted the last session. Of the resulting 93 sessions, 41 had color differences. Subjects held the key (and therefore looked at the colors) significantly longer in the case of a color difference ($\bar{x} = 954\ ms; se = 134\ ms$) than in the case without a color difference ($\bar{x} = 553\ ms; se = 9\ ms; R^2 = 0.05; F(1, 1137) = 60.9; p < 0.001$).

Subjects did not reject a connection when no color difference occurred. Two subjects missed color differences, one twice, which yields a false acceptance rate of 7.1%. This is higher than the false acceptance rates of the secure pairing methods studied by Uzun et al. in [31], which were zero and five percent. However, some closer look at the falsely accepted sessions is warranted.

Subject one encountered the color difference on the 14th key

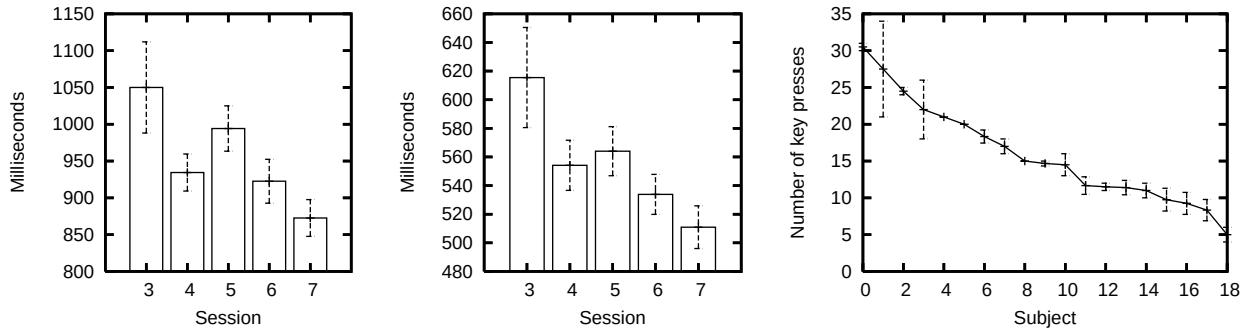


Figure 5: (Left) Shows the mean time with standard error from one key press to the next by session. (Middle) Shows the mean time and standard error for which subjects held the key down by session. (Right) Shows the mean number of clicks and standard error for each subject.

press in the first session that counted for the study. The time she depressed the key (and the colors were displayed on screen) decreased constantly from 600 ms to 196 ms in the second to last round and to 164 ms in the last round, in which the color difference occurred. Subject two accepted all sessions despite having two sessions with attacks. On average, this subject depressed the key for the shortest amount of time with very little variance ($\bar{x} = 236\ ms; sd = 42$).

In terms of average completion time, the methods studied by Uzun et al. appear to have a slight advantage. Six digits amount to about 20 bits worth of uncertainty, which would require an entry time of roughly 18 seconds in our mechanism, considering learning. The secure pairing methods studied by Uzun et al. took between 13 and 16.4 seconds on average [31].

The left and middle graphs in Figure 5 show how long the time was from one key press to the next (about 1 second) and how long keys were depressed (about half a second). Both results show a clear learning effect. With increasing number of sessions, subjects became faster at perceiving the colors and making their decisions. The average number of key presses with the standard error is given by subject in the rightmost graph in Fig. 5.

Half of the subjects performed 15–30 comparisons and the other half performed 5–14 comparisons. For this statistic, we counted only the sessions in which subjects accepted the connection.

Correlations

We did not find age or gender effects. Ease of use was correlated with professionalism as reported above. Subjects who thought the mechanism easy to use also felt that it did not require a lot of mental work ($r = -0.75; t = -4.61; p < 0.001$). When subjects felt that click sequences were too long they also had less confidence that they had not overlooked any color differences ($r = -0.7; t = -4; p < 0.001$) and regarded the mechanism as less professional ($r = -0.66; t = -3.58; p < 0.005$).

4.3 Interpretation

Subjects generally responded favorably to our mechanism. In sessions without attacks, subjects clicked more than 14 times on average. The resulting level of security should be good enough for most situations. If higher levels of security are required then this is accomplished easily and efficiently.

The false acceptance rate appears high at first glance. However, the sample size is small and closer examination of the data suggests that the subjects who account for all errors were not paying close attention to the task when the color differences occurred. While subjects agreed to participate in the study they may have hurried through the task without due diligence. We expect users behave more diligently when their actual assets are at risk.

5. CONCLUSIONS AND FUTURE WORK

We developed a simple and effective protection mechanism, which helps users to ascertain that they do not connect to evil twin wireless access points in public places such as cafés. The mechanism has minimal user interface requirements and can be implemented cheaply on a wide range of mobile and wireless devices. We built a proof of concept implementation and conducted a user study with it in a number of cafés in Palo Alto and San Francisco. The results of our study lead us to conclude that our protection mechanism can be deployed successfully. However, users must be willing to utilize the mechanism diligently. In those cases were we observed false acceptance of attacked session, our data suggests that subjects were not incapable of performing but were operating carelessly. As future work we would like to compare our mechanism directly with other methods such as the ones studied by Uzun et al. in [31]. Should this study be successful it would be interesting to build a higher fidelity prototype and to test it in the course of a field study.

Acknowledgments

Many thanks to John Adcock, Maribeth Back, Tony Dunnigan, Gene Golovchinsky, Don Kimber, Pernilla Qvarfordt for helpful suggestions, as well as all of the participants in our study. We are grateful to FXPAL for supporting this research.

6. REFERENCES

[1] ABDOLLAH, T. Ensnared on the wireless Web. Los Angeles Times, March 16 2007.

[2] ALKASSAR, A., STÜBLE, C., AND SADEGHI, A.-R. Secure object identification: or: solving the chess grandmaster problem. In *NSPW '03: Proceedings of the 2003 workshop on New security paradigms* (New York, NY, USA, 2003), ACM Press, pp. 77–85.

[3] BALFANZ, D., SMETTERS, D. K., STEWART, P., AND WONG, H. C. Talking to strangers: Authentication in ad-hoc wireless networks. In *Proceedings of Network and Distributed System Security Symposium 2002 (NDSS'02)* (San Diego, CA, February 2002).

[4] BIBA, E. Does your Wi-Fi hotspot have an evil twin? PC World, March 15 2005. Author writes for Medill New Service.

[5] BRANDS, S., AND CHAUM, D. Distance-bounding protocols. In *EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology* (Secaucus, NJ, USA, 1994), Springer-Verlag New York, Inc., pp. 344–359.

[6] BUSSARD, L., AND ROUDIER, Y. Embedding distance-bounding protocols within intuitive interactions. In *Proc. Conference on Security in Pervasive Computing (SPC'03)* (Mar. 2003), vol. 2802 of *Lecture Notes in Computer Science*, Springer Verlag, pp. 143–156.

[7] DOHRMANN, S., AND ELLISON, C. Public-key support for collaborative groups. In *Proc. 1st Annual PKI Research Workshop* (Gaithersburg, Mayland, USA, Apr. 2002), National Institute for Standards and Technology, pp. 139–148.

[8] FLEISHMAN, G. My evil twin. Published online at `http://wifinetnews.com/archives/004718.html`, January 20 2005.

[9] GEHRMANN, C., MITCHELL, C. J., AND NYBERG, K. Manual authentication for wireless devices. *RSA Cryptobytes 7*, 1 (Jan. 2004), 29–37.

[10] GOODRICH, M. T., SIRIVIANOS, M., SOLIS, J., TSUDIK, G., AND UZUN, E. Loud And Clear: Human verifiable authentication based on audio. In *Proc. 26th International Conference on Distributed Computing Systems* (July 2006), IEEE.

[11] GROUP, T. S. Airsnarf. Published online at `airsnarf.shmoo.com`, Apr. 2007. Airsnarf is a simple wireless access point setup utility designed to demonstrate how a rogue access point can steal usernames and passwords from public wireless hotspots.

[12] HALLER, N., METZ, C., NESSER, P., AND STRAW, M. A one-time password system. Internet Request for Comments 2289, Internet Engineering Task Force, Feb. 1998.

[13] KUO, C., WALKER, J., AND PERRIG, A. Low-cost manufacturing, usability, and security: An analysis of Bluetooth simple pairing and Wi-Fi protected setup. In *Proc. Usable Security Workshop (USEC)* (Lowlands, Scarborough, Trinidad/Tobago, Feb. 2007). Co-located with 11th Conference on Financial Cryptography and Data Security.

[14] LAUR, S., AND NYBERG, K. Efficient mutual data authentication using manually authenticated strings. In *Proc. 5th International Conference on Cryptology and Network Security* (Suzhou, China, 2006), no. 4301 in Lecture Notes in Computer Science, Springer Verlag, pp. 90–107.

[15] LIKERT, R. *A technique for the measurement of attitudes*. McGraw-Hill, New York, USA, 1932.

[16] MAHER, D. P. Secure communication method and apparatus. United states patent 5,450,493, United States Patent and Trademark Office, Sept. 1995. Filed Dec. 29, 1993.

[17] MCCUNE, J. M., PERRIG, A., AND REITER, M. K. Seeing-Is-Believing: Using camera phones for human-verifiable authentication. In *IEEE Symposium on Security and Privacy* (2005), pp. 110–124.

[18] MEADOWS, H. "Evil Twin" hotspots are a new menace for internet users, warns cranfield university. Press release, Cranfield University, Cranfield, Bedfordshire, MK43 0AL, United Kingdom, Jan. 2005. Available online at `http://www.cranfield.ac.uk/university/press/2005/14012005.cfm`.

[19] MILLER, G. A. The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review 63* (1956), 81–97.

[20] ORNAGHI, A., AND VALLERI, M. Ettercap. Available online at `ettercap.sourceforge.net`, Apr. 2007. Ettercap is a network sniffer with extensive support for Man-in-the-Mddle Attacks.

[21] PERRIG, A., AND SONG, D. Hash visualization: a way to improve real world security. In *International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99)* (1999).

[22] REKIMOTO, J., AYATSUKA, Y., AND KOHNO, M. SyncTap: An interaction technique for mobile networking. In *Human-computer interaction with mobile devices and services (Mobile HCI 2003)* (2003), L. Chittaro, Ed., no. 2795 in Lecture Notes in Computer Science, Springer Verlag, pp. 104–115.

[23] RICHARD, G. G. Service advertisement and discovery: Enabling universal device cooperation. *IEEE Internet Computing 4*, 5 (2000), 18–26.

[24] SALTZER, J. H., AND SCHROEDER, M. D. The protection of information in computer systems. *Communications of the ACM 17*, 7 (July 1974).

[25] SASTRY, N., SHANKAR, U., AND WAGNER, D. Secure verification of location claims. In *Proceedings of the 2003 ACM workshop on Wireless security (WiSe'03)* (New York, NY, USA, 2003), ACM Press, pp. 1–10.

[26] SAXENA, N., EKBERG, J.-E., KOSTIAINEN, K., AND ASOKAN, N. Secure device pairing based on a visual channel. In *IEEE Symposium on Security and Privacy* (May 2006).

[27] SHNEIDERMAN, B. *Designing the User Interface*, 3rd ed. Addison Wesley, 1998.

[28] STAJANO, F., AND ANDERSON, R. J. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proc. 7th International Security Protocols Workshop* (1999), pp. 172–194.

[29] SUOMALAINEN, J., VALKONEN, J., AND ASOKAN, N. Security associations in personal networks: A comparative analysis. Technical Report NRC-TR-2007-004, Nokia Research Center, Jan. 2007.

[30] THOMSON, I. "Evil Twin" Wi-Fi hacks target the rich. VNU Business Publications, November 23 2006. Available online at `www.vnunet.com/2169400`.

[31] UZUN, E., KARVONEN, K., AND ASOKAN, N. Usability analysis of secure pairing methods. In *Proc. Usable Security Workshop (USEC)* (Lowlands, Scarborough, Trinidad/Tobago, Feb. 2007). Co-located with 11th Conference on Financial Cryptography and Data Security.

[32] VAUDENAY, S. Secure communications over insecure channels based on short authenticated strings. In *Proc. Advances in Cryptology (CRYPTO)* (2005), vol. 3621 of *Lecture Notes in Computer Science*, Springer Verlag, pp. 309–326.

[33] ČAGALJ, M., CAPKUN, S., AND HUBAUX, J.-P. Key agreement in peer-to-peer wireless networks. *Proceedings of the IEEE 94*, 2 (Feb. 2006), 467–478.

[34] VOGEL, E. K., AND MACHIZAWA, M. G. Neural activity predicts individual differences in visual working memory capacity. *Nature 428* (Apr. 2004), 748–751.