Security Pairings using Physical Properties of Wireless Communication

Jani Suomalainen, Antti Evesti, Adrian Kotelba
VTT Technical Research Centre of Finland
Espoo and Oulu, Finland
{jani.suomalainen, antti.evesti, adrian.kotelba}@vtt.fi

***Abstract*—New security solutions in the physical communication layer – *secret key extraction from the radio channel* and *information-theoretic secrecy* – protect confidentiality of communication without cryptographic establishment of secret keys. Unfortunately, they currently lack authentication. Cryptographic mechanisms have still been needed to secure the first contact – to guarantee that security pairings between previously unknown devices are out of attackers reach. In this paper, we contribute by analyzing how five different security pairing approaches can be realized or complemented with physical layer solutions. We propose new solutions for replacing the use of expensive crypto algorithms with secret key extraction. We note that information-theoretic secrecy solutions are less capable of surviving without cryptographic protocols. However, we recognize one potential receiver-authentication approach for further studies: out-of-band delivery of channel state information.**

Keywords— wireless; authentication; security pairing; physical layer security; information-theoretic secrecy; key extraction

I. Introduction

Security pairing establishes a secure connection between two previously unknown wireless devices. Existing pairing mechanisms typically rely on end-users' assistance to point out which device is paired with which one. For example, to pair two smart phones the end-user may need to type a password or to physically connect them (by touching one device with another or by connecting them with a cable). When devices are communicating, they use *authentication* protocols to ensure that the received information is coming from a paired transmitter. Traditional pairing and authentication solutions are based on cryptographic key establishment protocols.

Recent physical layer security solutions – *secret key extraction from the radio channel* [1–3] and *information-theoretic secrecy* [4, 5] – promise confidentiality without establishing secret keys with cryptographic protocols. These mechanisms, recapitulated in Section II, utilize characteristics of wireless communication, such as disturbances, noise, and fading of radio signals, to prevent eavesdropping. However, these solutions do not authenticate previously unknown devices; the end-user cannot be sure that the paired devices have a direct security relationship between them and not with the man-in-the-middle attacker who eavesdrops or modifies transmissions. Hence, designers of wireless systems are still stuck with cryptographic pairing and authentication algorithms and with their problems – requirements for large computing and communication capacity and reliance on unproven assumptions that asymmetric functions are hard to solve.

In this paper, we explore the relationships between different pairing and physical layer security approaches. We asked whether physical layer solutions can be used to replace more expensive cryptographic protocols. We analysed, in Section III, how secret key extraction and information-theoretic secrecy approaches can support common pairing models, which are based on passwords, short-strings, certificates, out-of-band channels, or which are unauthenticated. We propose new approaches and protocols for implementing security pairing by replacing or complementing cryptography with physical layer security.

II. Physical Layer security

A. Key Extraction from the Radio Channel

Physical layer key extraction solutions – seminally described by Hershey et al. [1], Azimi-Sadjadi et al. [2] and Mathur et al. [3] – establish a secret key for two devices by utilizing location-specific and reciprocal characteristics of wireless channel. Wireless signals are location-specific as they travel through multiple paths and face different obstacles – buildings, people, vehicles – causing the signal to slightly fade and distort. Signals travelling different paths rapidly decorrelate from each other when the distance between them increases. Wireless signals are also reciprocal, which means that the electromagnetic wave propagation is identical in both directions. Hence, the wireless channel is similar for both sides nevertheless of which party initiates the communication. By recording fluctuations in signal amplitude and phase at the same time, two communicating devices may extract entropy measurements, which are random and available only for these devices. This information can then be used to generate secret keys.

Recently, several researchers further developed fast key extraction techniques for different networks. Jana et al. [6] studied and improved the performance of key extraction mechanisms. They noted that in stationary environments the amount of entropy is small and that fast key generation requires changes in the environment. Wang et al. [7] proposed fast techniques for group key generation. Gollakota et al. [8]

proposed retransmissions by the sender and jamming by the receiver in order to increase the key extraction speed and were able to achieve the secrecy rate of 3-18 Kb/s.

The existing proposals for key extraction are unauthenticated; two communicating parties, Alice and Bob, cannot be sure that they are establishing keys with each other and not with an attacker Mal. After key extraction, the extracted keys can be used to authenticate the subsequent communication between devices by using any cryptographic authentication protocol, which is based on symmetric keys. New keying material can be generated all the time to enable keys to be changed according to the needs of protocols. Also, as noted by Clark [9], the key extraction solutions may be combined with device fingerprinting techniques (see Subsection II.C) to identify the device. However, extracted keys or fingerprints are not enough for pairing; the devices first need to learn which keys or fingerprints belong to the intended devices.

An observation that characteristics of radio signals correlate with distance can be used to prove proximity of devices. Varshavsky et al. [10] utilize this observation for pairing wireless devices. The solution – Amigo – uses characteristics of radio signals to verify that devices are in close proximity to each other. In Amigo, two devices first establish a Diffie-Hellman key and then share received signal strength measurements they record from the radio environment. The pairing is accepted if a received measurement is similar to device's own recordings. In another pairing solution – ProxiMate by Mathur et al. [11] – two devices, in close proximity, measure variations in phase and amplitude of signals from third-party transmitters. Then they generate a secret key from these measurements. An eavesdropper within longer distance cannot establish the same key since the correlation between measurements taken by devices decreases when the distance between two devices increases. The proximity based pairing solutions assume that the paired devices can be kept very close to each other and that attackers are distant.

B. Information-theoretic secrecy

Information-theoretic secrecy approaches attempt to make eavesdropping impossible by arranging communication so that the signal-to-noise ratio (SNR) is large for legitimate communication between Alice and Bob and, simultaneously, SNR for eavesdropper Eve is small. Theoretical foundations for information-theoretic secrecy were presented by Shannon [4] already in 1940's and were later on extended by Wyner et al. [5] with a wiretap channel model. Information-theoretic security utilizes fading and difference effects in signals travelling different paths. In practise, it is achieved with secrecy coding (e.g. [12–14]) and beamforming (e.g. [15, 16]) techniques (which minimize the interference for legitimate communicating counterparties and maximize interference for others) and by adding artificial noise to the channel (to distract third-party eavesdroppers) [17]. Parameters, needed in these techniques, are selected by using channel state information (CSI), which in existing approaches are collected when Alice and Bob initiate or adjust their channel and which are assumed to be trustworthy. Eavesdropper may try to affect CSI in order to impair information theoretic secrecy e.g. by contaminating pilot signals [18] or tampering feedback channel.

Information-theoretic secrecy provides confidentiality by protecting communication from eavesdropper. However, it does not provide authenticity. It does not guarantee that Alice initiates communicating with Bob instead of Mal. In addition, Mal may try to initiate session hijacking at any time during communication. For instance, Mal, who is assumed to know the transmission frequencies and time slots used by Alice and Bob, may transmit at those slots using her own stronger signal to modify transmitted information. For authenticity, alternative mechanisms (based e.g. on cryptographic protocols and shared keys) are needed. If devices do not share a secret key, they can agree it at the beginning of their interactions to prevent session hijacks.

C. Fingerprinting

Devices can be identified by monitoring unique properties of their radio signals. Even when transmitting the same information and using same kind of transmitter hardware, signals have unique identifiable characteristics due to transmitter's hardware imperfections and location. The fingerprinting can be based on the following techniques:

- *Radio frequency (RF) fingerprinting* [19, 20] is a method of identifying radio transmitters' hardware with a low-error probability by measuring e.g. frequency and amplitude of signal transients. Each transmitter has unique rise time fingerprint when it starts a transmission. This uniqueness is caused by the slight variations of component values during manufacture. This fingerprint depends of various sources, including characteristics of frequency synthesis systems, modulator subsystems, and RF amplifiers.
- *Location fingerprinting* is a method for determining the location of the transmitter. The location can be resolved from different signal factors including the angle of arrival [21]. RF fingerprints are also dependent on the location making replaying of fingerprints more difficult [22].

III. Pairing Models With Physical Layer Security

This section surveys different security pairing models, which have been adopted to different standards including Bluetooth Secure Simple Pairing [23], WiFi Protected Setup [24], and Wireless USB Association Models [25]. The focus is on the user experience that these models provide. Then for each surveyed model we analyze how it can be realized or enhanced with physical layer security solutions.

A. Password-based Pairing

1) Overview

A secret password is widely used authentication mechanism in short-range wireless networks. For example, when bringing a new device to a network, the end-user is required to enter a password, which in WiFi must be 8 to 63 ASCII characters and in Bluetooth typically 4 digits. Usually, the end-user is required to preconfigure a password to another device, e.g. access point, in advance when it is first deployed. Alternatively, the key is configured in the factory as with older Bluetooth peripherals without proper I/O capabilities.

A password is used only when devices are connected for the first time; symmetric key derivation functions build sessions keys from a pre-shared key to be later on used with message authentication and encryption. Communication for (mutual) authentication occurs through untrusted (in-band) channel. Essential components and an example notification, displayed for the user, are illustrated in Fig 1.

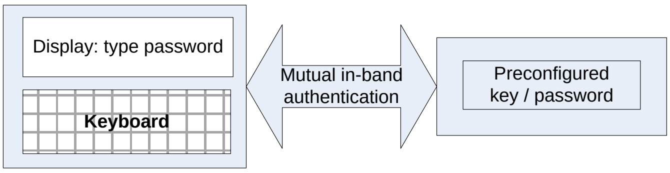

Fig 1. Authentication through pre-shared keys.

The security level of a password system can be increased with additional controls. For instance, the amount of password guesses can be controlled by monitoring and limiting requests. One time passwords increases the secrecy level significantly; the attacker is not able to launch password guessing attacks and the amount of cipher text material that the attacker is able to get is limited. However, one-time password must be acquired from an external source. In other words, the user is required to have an additional device, which limits the feasibility of such solutions.

Protection against passive dictionary attacks can be achieved with advanced crypto solutions, which cause significant costs in terms of time and resource consumption. For instance, Encrypted Key Exchange (EKE) [26] and, widely adopted, Secure Remote Password (SRP) [27] protocols, prevent dictionary attacks by using a combination of symmetric passwords and asymmetric protocols.

2) Physical Layer Opportunities

Requirements for passwords and pre-shared keys are less demanding when they are used with **keys extracted** from the physical layer. By strengthening the authentication algorithm with physical layer key, a passive eavesdropper or an active man-in-the-middle attacker denied any useful authentication information. As only active guessing attacks must be addressed, passwords can be shorter without being weak.

The work amount of a successful *passive (off-line dictionary) attack* depends on the key size. When the key is derived from the password, the attacker must try at maximum $pwcharset^{passlen}$ times (where *pwcharset* is amount of different possibilities for one password letter and *passlen* is the length of password). Hence, the success probability of the password guessing attack is $t/pwcharset^{passlen}$, (where *t* is the amount of guesses the attacker has). For instance, if the password is eight characters (alphanumeric with 64 possibilities) long, the work amount and success probability of attacker to guess a password with probability one would be $2.8 * 10^{14}$ and $1/64^{8} \approx 1/(2.8 * 10^{14})$, respectively. However, if a key is derived both from the password and, e.g. 128 bit, physical layer key, the numbers would be $1/64^{8} * 1/2^{128} \approx 1/(9.5 * 10^{52})$ and $9.5 * 10^{52}$. Consequently, with simple password authentication schemes relatively long passwords or additional protection mechanisms are required. With key extraction enhanced password authentication, passive attacks are unpractical.

The work amount to perform a successful *active attack* depends on the password length. In active attacks, the wireless connection is created between the legitimate party (Alice) and attacker (Mal). The attacker knows the extracted key. Thus, the password must be strong enough to withstand guessing attacks. In many scenarios this is not as hard requirement as the attackers' capability for brute force online guessing can be limited. For example, one-time passwords and similar solutions prevent attacker from performing multiple online authentication guesses.

One simplified password authentication protocol is illustrated in Fig 2. The protocol uses keys extracted from the physical layer to thwart passive attacks and message authentication code (MAC) function to prevent man-in-the-middle (Mal) from resolving and reusing the password. The key extraction solutions provide forward-secrecy. Even if attacker can resolve one physical layer key or session key, the attacker cannot resolve password or previous session keys. Alice and Bob can continuously monitor wireless channel and extract new keys according to the needs of the security protocol.

1. Alice transmits her user id and a hash of password, key extracted from the physical layer and random nonce to Bob

   Alice->Bob: id_{Alice}, MAC(pwd_{Alice}, key_{physec}, $nonce_{1}$), $nonce_{1}$

2. Bob calculates a MAC from Alice's password, physical layer key and $nonce_{1}$. If calculated value equals data, which was received from Alice, Bob has authenticated sender as Alice.

3. Bob transmits his user id and hash of password, key extracted from the physical layer and random nonce to Alice

   Bob->Alice: id_{Bob}, MAC(pwd_{Bob}, key_{physec}, $nonce_{2}$), $nonce_{2}$

4. Alice calculates a MAC from password, physical layer key and $nonce_{2}$. If calculated value equals data, which was received from Alice, Alice has authenticated sender as Bob.

Fig 2. A password and key extraction based mutual authentication protocol, which is tolerant against passive dictionary and active man-in-the-middle attacks

Similarly, **information-theoretic secrecy** channels can be used to prevent passive eavesdropping attacks – to transmit a password confidentially. However, there is no defence against active attacks - a password may be transmitted to anyone. Consequently, in situations where an attacker may be present at the time of initial connection, information-theoretic secrecy alone is not a viable solution.

B. Short-string based Pairing Models

1) Overview

Typing a long password is cumbersome for the end-user and is not possible with small devices without keyboard. To address these problems research community has developed short-string [28–32] and short-secret [33, 34] based authentication protocols for short-range communication. Advantages, compared to traditional password are that passwords do not need to be necessarily inputted by the end-user and can be shorter (typically between 6 to 8 digits). A short-string needs to withstand only one active guess - not passive attacks. Furthermore, one-time used short-strings are not required to be confidential; an attacker does not get advantage of seeing the string at real-time. From the end-user perspective, two main variations of the model have been introduced:

1) In short-string compare model (illustrated in Fig 3), connected devices both display the string. The end-user is expected to compare that both devices show the same string and only then accept the security association. This model is suitable for devices that both have a display.

2) In short-string entry model, the end-user is required to type a short-string that is displayed by one device to another. The model is suitable for cases where only one device has a display and another has a keyboard.

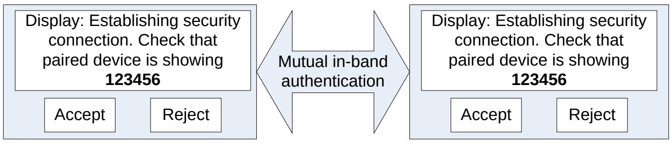
Display: Establishing security connection. Check that paired device is showing
123456
Accept
Reject
Mutual in-band authentication
Display: Establishing security connection. Check that paired device is showing
123456
Accept
Reject

Fig 3. Authentication by comparing short-strings

To agree a secret key using short-strings both devices need to exchange public keys and random values and one device a commitment to the random value [30]. After end-user has verified the short-string, which is derived from the public keys and random numbers, the two devices (knowing each other's public key) can execute some asymmetric key establishment protocol such as Diffie-Hellman.

2) *Physical Layer Opportunities*

Key extraction solutions can replace the cryptographic key establishment protocols that are used in short-string based pairing. The short-strings can be generated directly from physical layer keys that are extracted from the radio channel. Consequently, paired devices do not need to implement and execute cryptographic algorithms (which in case of short-strings involves asymmetric public-private key algorithms and in case of short-secrets also several rounds of communication [24, 34]).

A physical layer key is typically too long for the end-user to compare or type. Therefore, a short-string has to be derived from the extracted key using a particular short-string derivation function. This function should not give any clues of the extracted key for an attacker who can visually see the strings. Confidentiality of these strings itself is not a requirement (as it is not in existing short-string compare models either). Good candidates for such functions are the hash functions.

Fig 4 illustrates the key phases of solution. Phases 1 (key extraction) and 2 (key shortening) replace the traditional short-string key agreement protocols. Phase 3 and 4 (the user compares displayed keys) is similar in the traditional alternative. An essential enabler for using key extraction with the short-string authentication is the strong tie between key and the radio channel. Extracted keys depend of several factors including the properties of transmitter, receiver and environment. Therefore, an attacker (receiver or transmitter alone) cannot manipulate signal characteristics, extracted keys or short-strings.

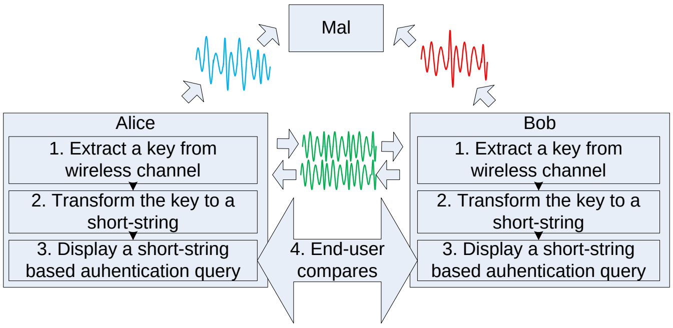
Mal
Alice
1. Extract a key from wireless channel
2. Transform the key to a short-string
3. Display a short-string based auhentication query
4. End-user compares
Bob
1. Extract a key from wireless channel
2. Transform the key to a short-string
3. Display a short-string based auhentication query

Fig 4. Extracting and generating short-strings for compare-based pairing. Alice and Bob extract keys from wireless (green) signals and generate short-strings from it. Mal sees decorrelated (blue and red) signals and cannot reproduce the key.

Information-theoretic secrecy does not provide the similar advantage as the key extraction approach, above. With secrecy coding there is no secret that the attacker could not reuse (if a secret key would be delivered from Alice through information theoretic secret channel, man-in-the-middle attackers could simply copy it and pass it to Bob). Therefore, 'traditional' short-string authentication protocols cannot be replaced.

C. *Out-of-band Pairing Models*

1) *Overview*

Out-of-band (OOB) pairing models [35, 36] enable devices to mutually authenticate by using a trusted channel. Existing OOB security realisations include WiFi Protected Setup, which defines a model providing the pre-shared key with a Universal Serial Bus (USB) stick; Bluetooth Secure Simple Pairing, which mentions Near Field Communication (NFC) as an example OOB channel; and Wireless USB (WUSB) Association Models, which enable security establishment by connecting devices with cables. In mobile networks, terminals are authenticated using symmetric keys stored in (U)SIM-cards, which can be considered as a one type of OOB channel.

Out-of-band channels may be one or two directional. Two directional channels, such as NFC and USB cables, enable devices to establish secrecy simply by transferring the key from one device to another. One-directional channels, such as RFID, USB memory sticks or light/camera combinations, require more complex protocols where OOB channel is used to transmit initial parameters for actual authentication occurring in in-band channel. For instance, in Bluetooth the OOB channel is used to transmit a secret - for the receiver to authenticate the transmitter – and a public key commitment – for the transmitter to authenticate the receiver. Particularly, the receiver signs its identifiers with the secret and verifies transmitter's public key, which is received from in-band channel, with the commitment (which is e.g. a signed hash of the public key).

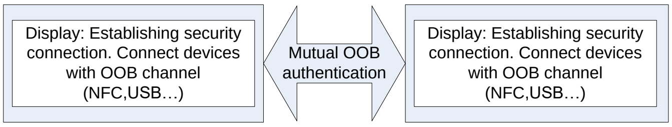
Display: Establishing security connection. Connect devices with OOB channel (NFC,USB…)
Mutual OOB authentication
Display: Establishing security connection. Connect devices with OOB channel (NFC,USB…)

Fig 5. Authentication with out-of-band (OOB) channel

2) Physical Layer Opportunities

Key extraction solutions can be applied with OOB pairing. In the protocol level use of physical layer keys changes the order of steps; now the symmetric key is extracted before OOB authentication. The implications for security protocol development depend on the OOB channel type:

- Two-directional unmodifiable OOB can be used to transmit to both directions a commitment to the extracted key (e.g. a hash of the key). The commitment proves that the devices, connected with OOB channel, know the same extracted key – No additional in-band message exchanges or public-private key pairs are needed. (Traditional approaches rely in this case on public-private keys).
- Two-directional OOB channels that are both confidential and unmodifiable can (as in traditional OOB channels) be used to transmit to both directions the extracted key or commitment to it (in the case bandwidth is an issue).
- One-directional OOB unmodifiable channels can be used to transmit a commitment to the extracted key (authenticating the transmitter for receiver) and a secret (a random value which the receiver can use to authenticate itself for the transmitter). Devices finalize the pairing as in traditional pairing approaches. Devices are not required to use public keys or asymmetric key agreement algorithms. (Traditional approaches rely in this case on public-private keys).

Information-theoretic secrecy solutions may use OOB channel as a control channel when adjusting channel parameters. In these cases OOB channel guarantees that the attacker is not able to tamper or eavesdrop channel status information (CSI) and hence affect coding or a radio parameter selection. Such OOB channel should provide be constantly available.

Fig 6 illustrates one scenario for dual-mode devices (Alice and Bob). These devices use high-capacity local area wireless network (protected only with information-theoretic secrecy) to transmit content and a network service (Charlie, which is accessed through a mobile network with cryptographic protection and authentication) as a control channel. In this scenario, the mobile network service, Charlie, is considered as a trusted OOB channel to mediate CSI. Alice uses these data to design a precoding, beamforming, and artificial noise approach for the channel between Alice and Bob. As a consequence, Mal cannot connect to Alice as channel negotiation and adjustment is based on CSI that cannot be tampered. To create such pairing, the end-user identifies mobile devices for the network service with some preregistered identifiers such as phone numbers.

Mal may try to manipulate channel conditions which Bob is detecting and indirectly affect to CSI. To succeed, Mal would need to generate such conditions which would make the channel available both for Bob and her. For instance, Mal could replace Alice’s pilot signals with her own low-SNR pilots, which would make Bob to request more transmission power from Alice. The used information-theoretic secrecy solution should make such attacks difficult (e.g. when signal strength is increased also artificial noise towards other locations is increased). To prevent session hijacking attempts, all CSI changes (e.g. due to movement) are delivered through trusted channel.

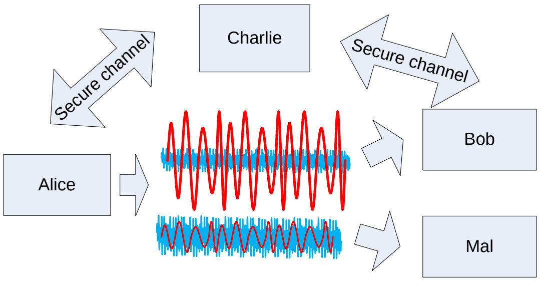

Fig 6. Agreeing information-theoretic secrecy (e.g. for local wireless) by sending control feedback through Charlie (e.g. through authenticated mobile network service). Alice and Bob agree channel with signal-to-noise ratio (red=data signal, blue=noise), which is good for Alice and Bob and bad for others.

The proposed solution can be used for *authenticating the receiver*. However, the transmitter is not authenticated. Mal may replace Alice’s signal with her own signal, which is visible for everybody including Bob. Consequently, the proposed approach is suitable for access control solutions i.e. for ensuring that only authorized user can access particular information. It is not suitable for cases where correctness of information (authenticity and integrity) is critical.

The solution can be applied with different kinds of secure (OOB) channels. Mobile network alternative is good candidate when the trusted authentication relationship exists with the devices and mobile operator. NFC may practical if the capacity of information theoretic secrecy channel is large than the capacity of NFC. Also, it may be possible to establish a cryptographic channel using keys extracted from the physical layer (e.g. with authentication mechanisms described in previous subsections) and using this channel to transmit the keys. However, establishment of a new cryptographic channel should not reveal CSI that the attacker can use to attack against information theoretic secrecy channel.

D. Trusted Parties and Certificate based Pairing Models

1) Overview

Certificates and public-private key pairs are typically used in mobile networks to authenticate a base station and in enterprise-level to authenticate WiFi clients. They can be used in approaches where there is a trusted party that is able to verify and certify devices. A typical trusted party solution uses certificates (to verify identities counterparties with particular private keys) and asymmetric cryptography (to establish symmetric session keys with these private key holders).

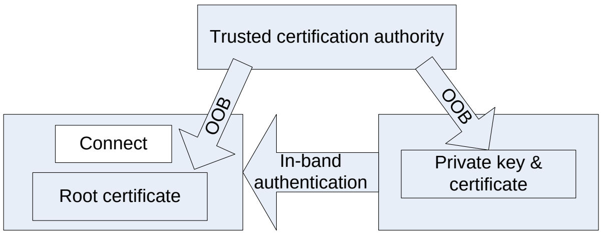

Fig 7. Authentication based on certificates and public-private key pairs

2) Physical Layer Opportunities

Certificates and public-private key pairs can be used to authenticate **keys extracted from the physical layer**. Authenticity of session keys must however be proven with certificates and asymmetric protocols regardless of the way they are created. This can be done e.g., as presented in Fig 8, by signing the session key with a certified private key in one device and then verifying these signatures in another. The approach is very similar when compared to traditional certificate based authentication; however now Alice does not generate a session key but uses the extracted key.

1. Bob receives Alice's public key ($PubK_{Alice}$) from a trusted party (Charlie) typically through a certificate

   Charlie => Bob: $PubK_{Alice}$

2. Alice and Bob agree a session key (K_{physec}) by extracting it from the physical layer

3. Alice signs the session key with her private key (PK_{Alice}) and sends the key to Alice

   Alice -> Bob: sign(PK_{Alice}, K_{physec})

4. Bob checks that the signature matches to Alice's public key by comparing it against the physical layer key.

   verify($PubK_{Alice}$ sign(PK_{Alice}, K_{physec})) == K_{physec}

Fig 8. A protocol for authenticating Alice to Bob based on certificates and keys extracted from the physical layer

Information-theoretic secrecy solutions cannot use certificates without additional authentication protocol for ensuring the authenticity of communication. The authentication protocol may be a cryptographic (asymmetric) protocol or a protocol based on key extraction (as presented in the previous paragraph).

E. Unauthenticated 'Push Button' Pairing Models

1) Overview

Unauthenticated 'push button' models pair devices easily with minimal hardware requirements. End-user's assistance is only needed to condition devices into a pairing mode – by pressing a button. Conditioned devices automatically establish secret keys with any other (conditioned) device they see. Examples of such models include 'push button' model in WiFi Protected Setup or 'just works' model in Bluetooth Secure Simple Pairing. They provide superior user experience and cost-efficiency when compared to user assisted key establishment models. However, these mechanisms are vulnerable against man-in-the-middle attacks – the end-user cannot control with whom a device establishes a secret key. The only protection is that the devices pair only during a limited time, e.g. a minute, and if multiple connection requests (potential attacks) are seen at that time the pairing is automatically aborted.

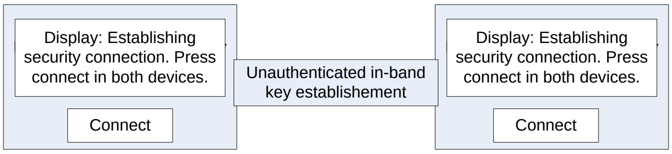
Display: Establishing security connection. Press connect in both devices.
Connect
Unauthenticated in-band key establishement
Display: Establishing security connection. Press connect in both devices.
Connect

Fig 9. Unauthentic security setup with 'push-button' model

2) Physical Layer Opportunities

Fingerprinting of wireless signals provide some opportunities to strengthen the 'push-button' pairings. Signal fingerprinting scenarios can be used to create an early locking between devices to prevent attackers from hijacking the channel. The strengthened protocol is the following: Alice records Bob's fingerprint and Bob records Alice's fingerprint when devices are starting the pairing and when the pairing is finalized. If Alice or Bob notice that the fingerprint has changed, the pairing is aborted and, if possible, an alternative stronger pairing mechanism is required.

Mal may attack such fingerprinting system in two ways:

1. She may copy Alice's fingerprint and use it when communicating with Bob and vice versa. The strength of solutions is based on the assumption that forging or replaying fingerprints is not easy. The replaying should be more difficult in pairing scenarios where at least the one party is knew and Mal has not time to gradually improve the security. Forging of RF fingerprints should be difficult at least with existing off-the-self hardware. As fingerprints depend also on environment, forging and replaying Alice's fingerprints is assumed to be difficult when Mal is in different location than Alice and, particularly, when Mal does not know Bob's location.

2. She may replace Alice's fingerprint with her own e.g. by transmitting at the same time as Alice w.g. but with stronger signal strength. However, as Mal cannot anticipate when a reference signal is recorded, she must be doing impersonation actively all the time (whereas in the un-strengthened solution, the attacker can just listen for a victim to initiate key establishment process and then intercept). Consequently, attacks against strengthened solution are easier to detect by Alice (or by some other device in the network detecting any changes in Alice's fingerprints).

Consequently, fingerprinting provides additional security for unauthenticated pairing mechanism. Particularly, it makes attacks trying to jam or tamper legitimate pairing signals more difficult. However, it cannot provide strong security against attackers with large resources.

IV. Discussion and Conclusions

We analysed five common models for pairing and authentication and discussed opportunities that physical layer security solutions can provide for them. In many practical pairing models, key extraction solutions can replace traditional asymmetric key agreement algorithms. Hence, physical layer security can reduce use and implementation of cryptographic algorithms. Particularly, key extraction solutions can replace asymmetric key agreement crypto algorithms, which are computationally expensive and whose security depends on unproven computational assumptions. The opportunities for each surveyed pairing solutions are summarized in the following table.

TABLE I. SUMMARY OF PHYSICAL LAYER POTENTIAL WITH DIFFERENT PAIRING MECHANISMS

Mechanism	Opportunities from the physical layer
Password	Extracted keys can protect passwords against passive attacks (removes need for protocols with more negotiations and asymmetric algorithms)
Short-string	Short-strings can be derived from extracted keys (removes need for protocols with more negotiations and asymmetric algorithms)
Out-of-band	1) Devices may exchange commitments to extracted keys using OOB channel (Removes need of asymmetric algorithms in 1 and 2 directional unspoofable (non-secret) OOB channels) 2) Information-theoretic secrecy channel may be authenticated using secure and authentic OOB channels carrying CSI
Certification	Asymmetric algorithms seem to be necessary for authentication. Extracted keys may be used as session keys.
'Push-button'	Device fingerprinting may be used as a one layer of protection against session hijacking attacks

While we emphasized the usefulness of key extraction solutions to prevent active man-in-the-middle attacks, we also noted that information-theoretic secrecy – confidentiality by secrecy coding – does not provide similar support for pairing or authentication solutions. Protection against man-in-the-middle attacks requires always some secret element that Mal cannot know (in traditional cryptography this element is the private key; in physical layer security it may be the shared (extracted) key). How to design and embed such a secret element into secrecy coding solutions remains an open question.

As one potential solution to authenticate information-theoretic secrecy (in a particular use case with dual-mode devices) we proposed a mechanism for reusing mobile network authentication. In more general, any existing authenticated secure channel may protect control information that is needed to achieve information-theoretic secrecy. At least as long as setting up the authentication channel does not compromise setting up of the information-theoretic secrecy channel. Hence, parameters for information-theoretic secrecy can be protected also with a cryptographic channel that is based on keys extracted from physical layer.

REFERENCES

1. Hershey, J.E., Hassan, A.A. & Yarlagadda, R. Unconventional cryptographic keying variable management. IEEE Transactions on Communications 1995, Vol. 43, No. 1, pp. 3-6.
2. Azimi-Sadjadi, B., Kiayias, A., Mercado, A. & Yener, B. Robust key generation from signal envelopes in wireless networks. Proceedings of the 14th ACM conference on Computer and communications security. 2007. Pp. 401-410.
3. Mathur, S., Trappe, W., Mandayam, N., Ye, C. & Reznik, A. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. Proceedings of the 14th ACM international conference on Mobile computing and networking. San Francisco, California, USA, New York, NY, USA: 2008. Pp. 128-139.
4. Shannon, C.E. Communication theory of secrecy systems. Bell system technical journal 1949, Vol. 28, No. 4, pp. 656-715.
5. Ozarow, L. & Wyner, A. Wire-tap channel II. Advances in Cryptology. 1985. Pp. 33-50.
6. Jana, S., Premnath, S.N., Clark, M., Kasera, S.K., Patwari, N. & Krishnamurthy, S.V. On the effectiveness of secret key extraction from wireless signal strength in real environments. Proceedings of the 15th annual international conference on Mobile computing and networking. Beijing, China, New York, NY, USA: 2009. Pp. 321-332.
7. Wang, Q., Su, H., Ren, K. & Kim, K. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. INFOCOM, 2011 Proceedings IEEE. 2011. Pp. 1422-1430.
8. Gollakota, S. & Katabi, D. Physical layer wireless security made fast and channel independent. INFOCOM, 2011 Proceedings IEEE. 2011. Pp. 1125-1133.
9. Clark, M. Robust wireless channel based secret key extraction. Military Communications Conference. 2012. Pp. 1-6.
10. Varshavsky, A., Scannell, A., LaMarca, A. & De Lara, E. Amigo: Proximity-based authentication of mobile devices. In: Anonymous UbiComp 2007: Ubiquitous Computing. Springer, 2007. Pp. 253-270.
11. Mathur, S., Miller, R., Varshavsky, A., Trappe, W. & Mandayam, N. Proximate: proximity-based secure pairing using ambient wireless signals. Proceedings of the 9th international conference on Mobile systems, applications, and services. 2011. Pp. 211-224.
12. Thangaraj, A., Dihidar, S., Calderbank, A.R., McLaughlin, S.W. & Merolla, J. Applications of LDPC codes to the wiretap channel. Information Theory, IEEE Transactions on 2007, Vol. 53, No. 8, pp. 2933-2945.
13. Xiang He & Yener, A. Providing secrecy with lattice codes. Communication, Control, and Computing, 2008 46th Annual Allerton Conference on. 2008. Pp. 1199-1206.
14. Mahdavifar, H. & Vardy, A. Achieving the secrecy capacity of wiretap channels using polar codes. Information Theory, IEEE Transactions on 2011, Vol. 57, No. 10, pp. 6428-6443.
15. Romero-Zurita, N., Ghogho, M. & McLernon, D. Physical layer security of MIMO–OFDM systems by beamforming and artificial noise generation. Physical Communication 2011, Vol. 4, No. 4, pp. 313-321.
16. Anand, N., Lee, S. & Knightly, E.W. STROBE: Actively securing wireless communications using Zero-Forcing Beamforming. Proceedings of IEEE INFOCOM. 2012. Pp. 720-728.
17. Negi, R. & Goel, S. Secret communication using artificial noise. IEEE Vehicular Technology Conference. 2005. Pp. 1906.
18. Zhou, X., Maham, B. & Hjorungnes, A. Pilot contamination for active eavesdropping. Wireless Communications, IEEE Transactions on 2012, Vol. 11, No. 3, pp. 903-907.
19. Toonstra, J. & Kinsner, W. A radio transmitter fingerprinting system ODO-1. Electrical and Computer Engineering, 1996. Canadian Conference on. 1996. Pp. 60-63.
20. Danev, B., Zanetti, D. & Capkun, S. On physical-layer identification of wireless devices. ACM Computing Surveys (CSUR) 2012, Vol. 45, No. 1, pp. 6.
21. Xiong, J. & Jamieson, K. SecureArray: improving wifi security with fine-grained physical-layer information. Proceedings of the 19th annual international conference on Mobile computing & networking. 2013. Pp. 441-452.
22. Danev, B., Luecken, H., Capkun, S. & El Defrawy, K. Attacks on physical-layer identification. Proceedings of the third ACM conference on Wireless network security. 2010. Pp. 89-98.
23. Bluetooth Special Interest Group . Bluetooth 2.1. Specifications. 2007. https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=241363.

24. Wi-Fi Alliance . Wi-Fi Protected Setup. Web site, 2013, Available: http://www.wi-fi.org/knowledge-center/articles/wi-fi-protected-setup%E2%84%A2 [2013, 6/14] .

25. USB Implementers Forum . Wireless Universal Serial Bus. Specification 1.1. 2010. http://www.usb.org/developers/wusb/docs/.

26. Bellovin, S.M. & Merritt, M. Encrypted key exchange: Password-based protocols secure against dictionary attacks. Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on. 1992. Pp. 72-84.

27. Wu, T. . The SRP Authentication and Key Exchange System. IETF standard. 2000. http://tools.ietf.org/html/rfc2945.

28. Zimmermann, P. . Pgpfone: Pretty good privacy phone owner's manual, version 1.0 beta 5, appendix c. 1996.

29. Vaudenay, S. Secure communications over insecure channels based on short authenticated strings. Advances in cryptology–CRYPTO 2005. 2005. Pp. 309-326.

30. Laur, S. & Nyberg, K. Efficient mutual data authentication using manually authenticated strings. Cryptology and Network Security. 2006. Pp. 90-107.

31. Pasini, S. & Vaudenay, S. SAS-based authenticated key agreement. In: Anonymous Public Key Cryptography-PKC 2006. Springer, 2006. Pp. 395-409.

32. Cagalj, M., Capkun, S. & Hubaux, J. Key agreement in peer-to-peer wireless networks. Proceedings of the IEEE 2006, Vol. 94, No. 2, pp. 467-478.

33. Larsson, J. Higher layer key exchange techniques for bluetooth security. Open Group Conference, Amsterdam. 2001.

34. Gehrmann, C., Mitchell, C.J. & Nyberg, K. Manual authentication for wireless devices. RSA Cryptobytes 2004, Vol. 7, No. 1, pp. 29-37.

35. Stajano, F. The resurrecting duckling. Security Protocols. 2000. Pp. 183-194.

36. Balfanz, D., Smetters, D.K., Stewart, P. & Wong, H.C. Talking to Strangers: Authentication in Ad-Hoc Wireless Networks. Network and Distributed System Security Symposium. 2002.