Device Pairing at the Touch of an Electrode

Marc Roeschlin
Department of Computer Science
University of Oxford
marc.roeschlin@cs.ox.ac.uk

Ivan Martinovic
Department of Computer Science
University of Oxford
ivan.martinovic@cs.ox.ac.uk

Kasper B. Rasmussen
Department of Computer Science
University of Oxford
kasper.rasmussen@cs.ox.ac.uk

***Abstract*—Device pairing is the problem of having two devices securely establish a key that can be used to secure subsequent communication. The problem arises every time two devices that do not already share a secret need to bootstrap a secure communication channel. Many solutions exist, all suited to different situations, and all with their own strengths and weaknesses.**

In this paper, we propose a novel approach to device pairing that applies whenever a user wants to pair two devises that can be physically touched at the same time. The pairing process is easy to perform, even for novice users. A central problem for a device (Alice) running a device pairing protocol, is determining whether the other party (Bob) is in fact the device that we are supposed to establish a key with. Our scheme is based on the idea that two devices can perform device pairing, if they are physically held by the same person (at the same time). In order to pair two devices, a person touches a conductive surface on each device. While the person is in contact with both devices, the human body acts as a transmission medium for intra-body communication and the two devices can communicate through the body. This body channel is used as part of a pairing protocol which allows the devices to agree on a mutual secret and, at the same time, extract physical features to verify that they are being held by the same person. We prove that our device pairing protocol is secure in our threat model and we build a proof of concept set-up and conduct experiments with 15 people to verify the idea in practice.

I. Introduction

Device pairing is the process of bootstrapping secure communication between two devices that do not share any common secrets. Often the most challenging part of a device pairing protocol is to establish the identity of the other device, i.e., to make sure that one is establishing a key with the intended device and not someone else. For devices on the Internet this problem is addressed by relying on certificate authorities to certify the identities of hosts, providing a root of trust when establishing the identity of a communicating party. For smaller devices that do not necessarily have (or need) a certified global identity, certificate authorities are often not appropriate. Smaller devices instead often use short range radio technology like Bluetooth, and rely on a human to certify the validity to the other device when pairing, e.g., by visually comparing short strings on a screen, or by typing a number displayed by one device into the other. Such schemes require active participation from a human and the security guarantees provided by these protocols rely on the user performing the correct actions at the correct time. If the user makes any mistakes, the security guarantees of these protocols no longer hold.

In addition to human error, device pairing protocols also impose certain hardware requirements on devices. This is not a problem by itself, as all communication requires some form of hardware support, but screens and input devices place restrictions on the size and shape of devices, e.g., a device may have to have a flat surface, and be big enough to support a usable screen.

In this paper we propose a device pairing protocol for small devices (e.g., phones, headsets, keyboards, etc.) that mitigates these two problems. Our protocol does require human participation but the user never has to make a security relevant decision and the hardware needed for communication can be any conductive surface on the device. This eliminates the possibility of human error and the scheme remains usable regardless of the physical design of the device (as long as the device is big enough to touch with a finger).

Our scheme is based on the core idea that two devices are allowed to be paired if they are both held by the same human, at the same time. The rationale behind this decision is that if a user is physically holding both devices there are very few ways to secure communication between these devices if the user has malicious intentions. For example a malicious user could run a device pairing protocol involving short string comparison (or any other mechanism), or physically manipulate the devices to achieve his goal. Our scheme enables device pairing by having the user touch a conductive surface on each device. The human body then serves as a transmission medium for capacitive coupling between the devices which can be used for communication. We call this communication channel the "body channel". Devices can distinguish between messages sent on this body channel, and messages sent by a remote attacker, and can thus ignore any message that originates from an external source. This means that two devices held by a user effectively have an authenticated channel between them that can be used for key confirmation. Only a small amount of data is sent through the body channel, so device pairing is fast and easy.

We make the following contributions:

- We present our device pairing protocol that takes advantage of the body channel to quickly and securely

Network and Distributed Systems Security (NDSS) Symposium 2018
18-21 February 2018, San Diego, CA, USA
ISBN 1-1891562-49-5
http://dx.doi.org/10.14722/ndss.2018.23076
www.ndss-symposium.org

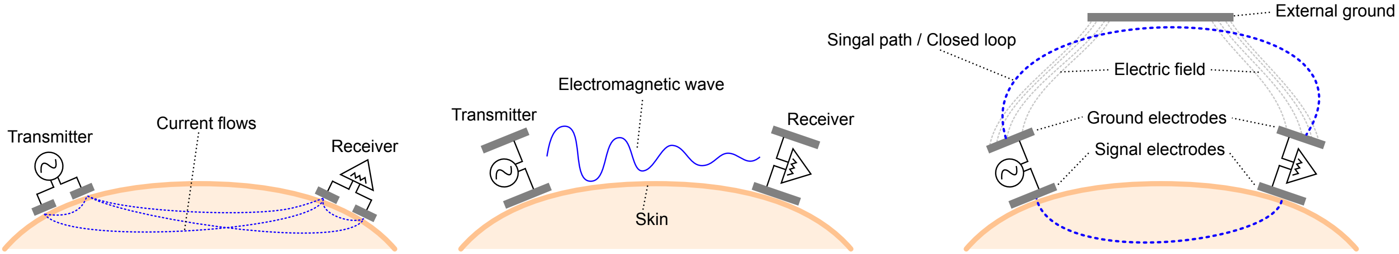

Fig. 1. Three main methods for intra- and on-body channel communication. From left to right: galvanic coupling, surface wave and capacitive coupling.

establish a shared secret, without the need for certificates or shared knowledge.

- We prove the security of our design. Specifically, we reduce the security of the protocol to the security of the underlying primitives under the assumption that the body channel is read-only to the attacker.
- The read-only assumption models the fact that the receiving device can tell the difference between messages sent by an external transmitter, and a device which is physically connected to the person performing the pairing. The receiving device can thus ignore any message that originates from an external source, which is equivalent to saying that the channel is read-only for the attacker. We present thorough experiments to verify this distinguishing ability.
- We design and implement a proof-of-concept prototype to conduct the experiments mentioned above and to experiment with performance and user experience.

II. Background on Intra-Body and On-Body Communication

Intra-body communication is a communication technique that transfers data wirelessly through the human body. Intra-body communication was first proposed in 1995 [38] and has since been covered in a large body of research literature: Numerous proposals on different transmission methods, receiver and transmitter types, as well as modulation techniques have been published, e.g., [8], [33], [37]. These and other promising results motivated the definition of intra-body communication as a physical communication layer in the relatively new IEEE 802.15.6 standard [17] which is the latest international standard covering Wireless Body Area Networks (BANs).

Even though said standard mentions medical and non-medical target applications for intra-body communication, the main drivers for the development of electric near-field communication in and around the human body have been the biomedical sciences and the medical field. Utilizing the body as a transmission medium for electrical signals is key to achieve low-power wireless sensors for (real-time) health monitoring [4], [13].

The main advantages for the use of intra-body communication over standard wireless communication for on- and in-body medical sensors is the high conductivity of the human body compared to air and the fact that most electromagnetic energy is not radiated into the environment, but confined through the body's surface, resulting in very low energy consumption [4]. Since most of the signal is restricted to the body area, external (radio frequency) interference does not affect the communication channel and robust data transmission can be realized without a large antenna.

Although these features could prove very useful for applications in the context of Computer Security, the use of the human body as a communication channel for security applications is largely unexplored. The possibility to transmit electrical signals through the human body while most energy is confined to the transmission medium should be of particular interest and is a property normally not found with other wireless communication techniques, such as Wi-Fi or Bluetooth. We test this property in detail in the experiments in Section VIII.

We will now briefly cover existing techniques for body channel communication to support understanding of our design choices in the following of this paper. Body-channel communication can be divided into roughly three groups:

a) Galvanic coupling: The concept of galvanic coupling is to induce alternating current into the human body. It was first proposed for intra-body communication in [36], [37] and it works by differentially applying a signal over two electrodes at the transmitter which will induce a current into the body. Both transmitter and receiver each have two electrodes that are coupled to the human body as shown in Figure 1. Most of the induced current flows directly from one sender electrode to the other, but a small portion propagates through the body to the receiver where it is detected as the voltage differential between the two receiver electrodes. The carrier of the information are the ionic fluids in the body that form a closed loop for signal transmission [30]. Advantages of galvanic coupling are virtually no "leakage" of the electric field outside of the body — galvanic coupling does not rely on electromagnetic transmission, but on electron flow — and the fact that no external ground reference is needed; the return path of the signal transmission is the human body.

b) Capacitive coupling: Capacitive coupling uses an electromagnetic signal for data transmission. The transmitter emits the signal through an electrode that is in touch with the human body. After having traversed the body, the signal is picked up by a receiver which is also coupled to the body (see Figure 1). The signal return path between transmitter and receiver is established though the environment by electrostatic coupling to external conductive objects, most often earth ground.

This type of communication is enabled by two physical properties: (1) At a frequency of less than 100 MHz, the wavelength of an electromagnetic signal is far greater than

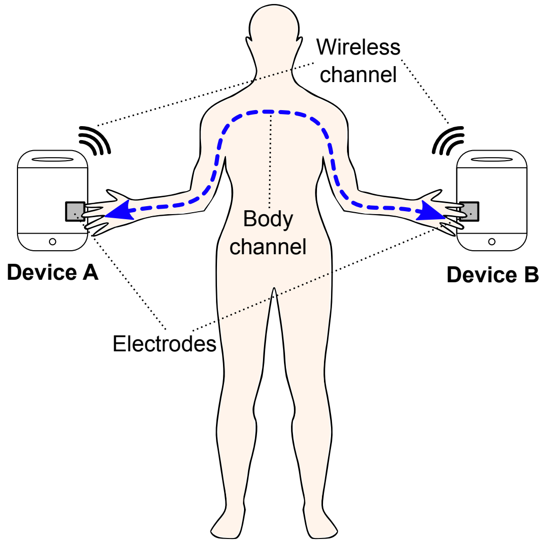

Fig. 2. A human pairs devices A and B. Both devices can communicate via a wireless channel and use the human body as a transmission medium for a second channel, the human body channel. The body channel is established by touching electrodes on both devices.

the size of the human body and the electric field around the body can be approximated as constant over time, i.e., the phase of the signal remains uniform anywhere close to the human body [3], and (2) the human body can be modeled as a conducting wire at low frequencies, i.e., capacitive near-field coupling establishes a closed loop for signal transmission [38].

c) Surface wave techniques: Surface techniques are often referred to as "on-body" or "near-body" transmission. They use higher frequencies than capacitive coupling and galvanic coupling. Most often frequencies on the order of more than 100 MHz are used. While some electromagnetic waves propagate through the body in a similar way as with capacitive coupling, usually, a significant amount radiates into the air [35]. In addition, as the signal propagates through the body it is attenuated considerably [3]. Unlike with capacitive coupling or galvanic coupling, there is no closed loop for signal transmission; the receiver just measures the intensity of the electromagnetic signal analogous to conventional radio frequency transmission.

III. Our Approach

The device pairing method we present in this paper relies on intra-body communication. The basic idea is that two electronic devices should be allowed to perform device pairing if they can successfully communicate with each other through a human body. The fact that two devices can transmit and receive messages using body communication implies that they must be physically close to each other and must be held by the same person. We use this as the criterion for whether two devices are meant to run a pairing protocol with each other and establish a mutual secret. A person can give two devices permission to pair by holding them both at the same time and thereby providing a transmission medium for intra-body communication.

Our proposed device pairing scheme uses capacitive coupling to establish the human body channel ("body channel"). Our choice to utilize this particular technique is founded on the following observations.

a) Transmission distance: The person pairing two devices should be able to touch them with their hands to perform the pairing. This requires hand-to-hand transmission on the body channel which can over 180 cm in adults. Capacitive coupling and surface waves are the only body communication techniques that have been reported to cover such a distance reliably. With galvanic coupling only short transmission distances are possible due to the high attenuation of the signal [4], [26]. In addition, the frequency ranges where galvanic coupling operates best are lower than for other techniques, which significantly restricts the data rate for communication [7].

b) Usability and electrode design: Capacitive coupling only requires one electrode per device to be in physical touch with the human body, i.e., the person pairing the devices only needs to touch one electrode with each hand. Unlike galvanic coupling, which requires at least two electrodes per device, capacitive coupling only uses a single capacitive touch-electrode per device. This simplifies the implementation of body channel enabled devices and makes the action of pairing two devices straightforward for the user. Additionally, the fewer electrodes there are, the less the effect orientation of transmitter and receiver have on the signal attenuation [18]. We elaborate on the design of the electrodes we used in our experiments in Section VII-B.

c) Electromagnetic interference: Surface wave techniques and capacitive coupling can both cover a transmission distance that is sufficient for our application with relatively little signal attenuation. Compared to capacitive coupling, surface wave techniques allow more electromagnetic power to leave the human body during transmission and are more susceptible to external interference. We aim to design body channel communication that is difficult to interfere with from the outside, i.e., with an external radio transmitter. It should require a lot of energy to influence the body channel with a signal source that is not physically connected to the body. Capacitive coupling, which operates at much lower frequencies than surface waves, is therefore better suited for our use case.

.

IV. System and Adversary Model

A. System Model

Two devices that do not share any secrets need to bootstrap secure communication. The devices follow the pairing protocol presented in Section V in order to agree on a mutual secret.

The decision whether two devices should be paired with each other and execute the pairing protocol is made by a human. A person can give the devices permission to run the pairing protocol with each other by physically touching and holding them both at the same time. Only if two devices are held by the same person they are allowed to be paired with each other. If a device is not connected with another device through a person, or if a device is not being held by a person at all, it should not be able to carry out the pairing process.

The devices each have an electrode that when touched by a human enables communication through capacitive coupling.

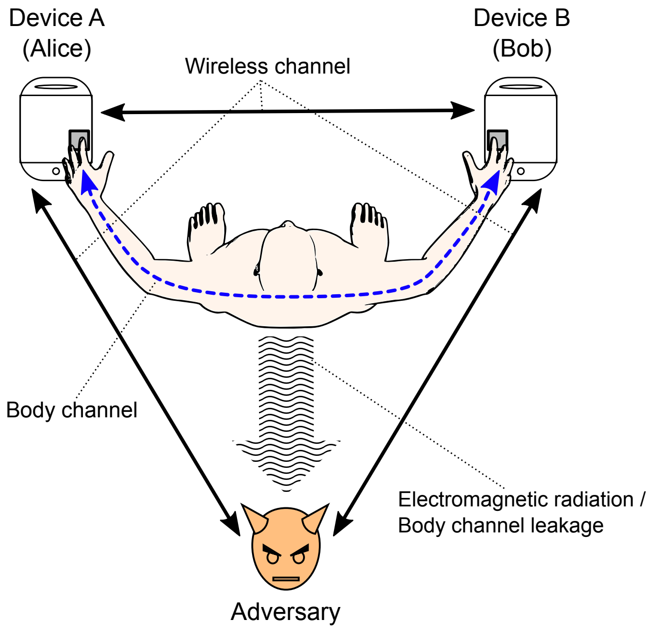

Fig. 3. An adversary interferes with the wireless channel and records the electromagnetic leakage from the human body channel.

We call this communication channel the *human body channel*. The devices can also communicate with each other on a *wireless channel* (see Figure 2). The wireless channel does not have to provide any particular security guarantees for the device pairing to work.

The human body channel is formed when a person is in physical contact with both devices. If a person touches both devices at the same time, one with each hand, the human body acts as a transmission medium for intra-body communication and both devices can send and receive messages on this channel. The human body channel also allows the devices to extract physical properties of received messages to validate if they have indeed been sent over the body channel, i.e., "through" the person who is currently touching both devices.

B. Attacker Model

We specify three different adversaries: An adversary who *eavesdrops* on the device pairing process, and adversary who tries to perform *remote pairing* with a body channel enabled device, and an adversary who launches a *man-in-the-middle attack* during the pairing of two devices.

- **Remote pairing.** This adversary tries to perform remote pairing with a body channel enabled device. The adversary does not have physical access to the target device and therefore can not authorize the device to pair by simply touching it. Due to the inability to touch or hold the target device, the adversary can not establish a body channel for the pairing process, but he can attempt to initiate the the device pairing by sending radio waves from a distance. He might do so while the target device is on its own or while a person is in physical contact with the device. It is important to consider such a scenario since a person could be touching the target device accidentally or be part of an ongoing pairing execution.
- **Passive eavesdropping.** This adversary listens on the wireless channel and records the electromagnetic leakage originating from the body channel (see Figure 3) in an attempt to learn about the secret that is being agreed on during the pairing of two devices.
- **Man-in-the-middle attack.** This adversary tries to actively participate in the pairing of two devices. His goal is that one or both of the devices believe the pairing protocol has completed successfully and the resulting secret is only known to the two devices. We make the assumption that such an adversary can relay, alter and inject messages on the wireless channel as well as record the electromagnetic signals transmitted on the body channel. In addition, the adversary can send electromagnetic signals at the the devices and the person involved in the pairing, but similarly to the remote pairing scenario, we assume that the adversary is not in physical contact with any of the two devices.

For all three adversaries, we assume that they can only establish an actual body channel if they are able to touch the devices or the person involved in the pairing. The devices can extract physical properties of the messages received on the body channel and detect with high accuracy if a message is an induced radio wave from an outside source. We thus consider the human body channel as read-only for any signal source other than the devices which are being paired and held by the same person. We show that this is a reasonable assumption in Section VIII. For the read-only property of the body channel to hold, we state a minimum distance of 50 cm between the adversary and the person involved in the pairing.

Like all other pairing protocols, our proposed pairing mechanism can not prevent denial of service attacks. Hence, we do not address attacks that have the sole goal of disrupting the communication between the devices.

V. Device Pairing Protocol

Two devices, henceforth referred to as Alice and Bob, jointly agree on a secret using a wireless channel and the human body channel. Alice and Bob follow the device pairing protocol outlined in Figure 4. If the protocol terminates, it guarantees that the secret is only known to Alice and Bob, provided they have not revealed it to any other party, of course. The resulting mutual secret can, for instance, be used in subsequent communication between the devices.

The protocol relies on the fact that Alice and Bob can independently verify if the messages they receive on the body channel have traveled through a human body. If they both conclude that the physical properties of the received messages match with the characteristics of the body channel, they must be communicating with each other through the same person. In that case, Alice and Bob must be held simultaneously by the same person and the pairing protocol can terminate successfully.

A. Protocol Description

The device pairing protocol consists of two steps: key agreement and key confirmation. Alice, who initiates the protocol, chooses a private key a and picks a random nonce

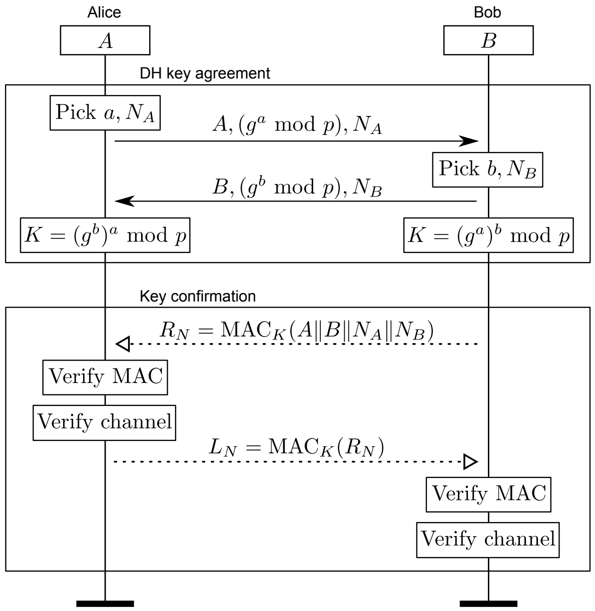

Fig. 4. The pairing protocol uses the wireless channel (solid arrows) for the key agreement and the body channel (dotted arrows) for the key confirmation.

N_A. She then sends her identity A, $(g^a \bmod p)$ and the freshly picked nonce N_A to Bob on the wireless channel. Bob then picks a private key b and a nonce N_B and sends his identity B together with $(g^b \bmod p)$ and the nonce back to Alice. Alice and Bob can now independently construct a mutual secret K and complete the key agreement phase. However, at this point, Alice and Bob can not yet be certain if K is indeed a mutual secret only known by them, since the wireless channel is unauthenticated.

The key confirmation phase follows immediately after the key agreement. Bob computes a message authentication code (MAC) R_N using the newly created key K (or a derivative thereof). The MAC is constructed over the concatenation of the identities and nonces, and is sent to Alice over the "body channel". Alice verifies the MAC R_N, and verifies that the message came through the body channel (as described in Section VIII). If both checks succeed, Alice knows that K is a freshly generated secret shared with Bob. By sending R_N to Alice, Bob demonstrates that he can transmit messages over the body channel and must be connected to Alice through the same human body. He also confirms that he knows K and proves that Alice must have been communicating with him in the preceding key exchange.

Finally Alice computes a MAC of R_N using K, and sends the result to Bob through the body channel. Bob verifies the MAC and the body channel like Alice did before. This proves to Bob that Alice is in possession of K and can transmit on the body channel.

Termination of the protocol guarantees that the mutual secret K is known to Alice and Bob, and only to them provided none of them revealed it to any other party. Moreover, Alice and Bob can be sure that they were both held by the same person when they ran the pairing protocol. If any of the verification steps fail, the protocol will terminate with an error.

VI. Security Analysis

The high-level goals of the adversary are to either eavesdrop on the traffic between two legitimate devices, place himself as a man-in-the-middle, or perform remote pairing with a target device.

In this section we show that neither a passive nor active adversary can achieve these goals. We assume that the adversary has full knowledge of the protocol including the public parameters g and p.

A. *Passive Eavesdropping*

To show that our device pairing protocol is secure against purely passive eavesdropping, we observe that the only information available to the adversary at the end of the key agreement part of the protocol are the identities of the two devices A and B, the freshly picked nonces N_a and N_B, as well as the public Diffie-Hellman parameters g^a and g^b. The identities are public and do not constitute information leakage. The two nonces are freshly picked independently from the private key, so they can not reveal any information. If the computational Diffie-Hellman assumption holds for the underlying group, then the adversary can not get the key K from this information.

Furthermore, we observe that the only additional information the adversary can obtain from the key confirmation part of the protocol are the two different MACs R_N and L_N. The MACs are computed using the key K (or a derived MAC-key), however assuming the MAC scheme is secure against existential forgery, R_N and L_N do not reveal information about the key.

B. *Remote Pairing*

In order for a remote adversary (i.e., an adversary that is not physically being held by the same human as the device) to perform device pairing, the adversary has to execute the protocol with an honest device. Without loss of generality we assume that the adversary takes the role of Alice, i.e., executes the protocol with Bob.

The adversary must proceed according to the protocol otherwise Bob will abort. After the key agreement part of the protocol, the adversary does indeed share a key $K' = (g^b)^{a'}$ with Bob. However, in the key confirmation part, after receiving $R_N = \mathrm{MAC}_{K'}(A\|B\|N_A)$ from the body channel, the adversary must send $L_N = \mathrm{MAC}_{K'}(R_N\|N_B)$ back on the body channel. By the read-only property of the body channel this can only be done with negligible probability (as explained in Section VIII), thus a remote attacker can not successfully complete the protocol with Bob (or Alice).

C. *Active Eavesdropping and Man-in-the-middle Attacks*

To demonstrate that our device pairing protocol is secure against an active man-in-the-middle attack, we observe the following. In order for the adversary to place himself in the middle between Alice and Bob, he must either run the protocol with each of them or interfere in an ongoing pairing session between Alice and Bob. Furthermore, the adversary must replace or modify at least one of the key agreement messages, as this would otherwise be passive eavesdropping.

TABLE I. PARAMETERS FOR INTRA-BODY COMMUNICATION USING CAPACITIVE COUPLING.

Parameter	Value
Frequency bandwidth	0.5 MHz - 3.5 MHz
Transmission distance	Hand-to-hand (180 cm)
Signal electrode	4 cm by 4 cm aluminum plate
Ground electrode	7 cm by 7 cm aluminum plate
Data encoding	Manchester code
Modulation scheme	On-off keying
Sending power	5 mW
Sender voltage	3 Vpp
Current through body	∼10μA

As we showed above for the remote pairing attack, the adversary can not successfully complete the protocol alone with either Alice or Bob. The protocol does not terminate in either case, since the body channel is read only for the adversary and thus the key confirmation fails.

Any modification of the public DH contributions g^a or g^b will, except with negligible probability, cause Alice and Bob to disagree on the key. For example, if the adversary replaces g^b with $g^{b'}$, we have

$$K_A = (g^{b'})^a \neq (g^a)^b = K_B,$$

which will result in the verification of R_N to fail in the key confirmation part. Interference with any of the other parameters sent in the protocol, A, B, N_A or N_B, will also cause the verification of R_N to fail, assuming the underlying MAC scheme is second pre-image resistant. By the read-only property of the body channel, the adversary can not modify or replace R_N. Nor can he replace L_N after Alice has aborted the protocol, as a result Bob will also abort.

The only remaining option for the adversary is to initiate two sessions simultaneously with both Alice and Bob, and then rely on them to complete the key confirmation phase. For this to succeed the adversary must create two sessions where all the nonces, identities and public parameters are the same, since these are inputs to the MAC-function in the key confirmation part of the protocol. If all parameters are identical in the two sessions, and Alice and Bob are both being held by the same human, the protocol would succeed, but the adversary would just have done passive eavesdropping (and learned nothing as shown above).

D. The Human Body Channel

The security of the protocol relies on the assumption that the human body channel is read only for the adversary. This assumption models the fact that the receiving device can tell the difference between messages sent by an external transmitter and a device which is physically connected to the person performing the pairing. The receiving device can thus ignore any message that originates from an external source, which is equivalent to saying that the channel is read only.

In the following sections we will document experiments that verify this particular channel property and we state the assumptions that need to be made in order for the property to hold.

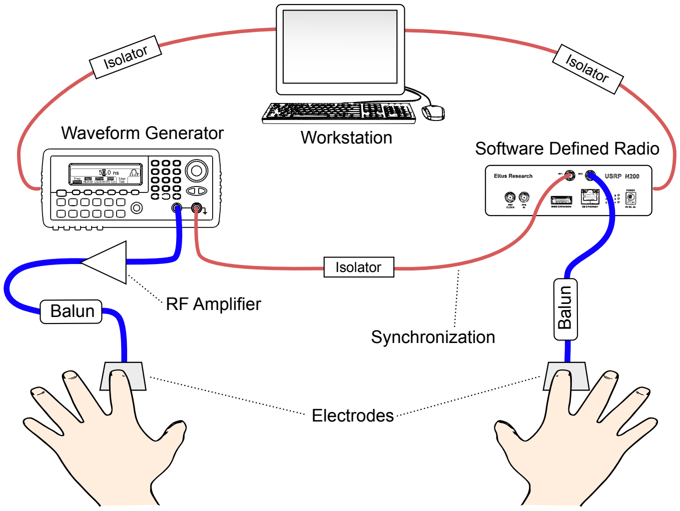

Fig. 5. Measurement setup. A waveform generator transforms the message into an electric signal which is amplified and emitted through the touch-electrode of the transmitter. The touch-electrode of the receiver is connected to a software defined radio which captures the incoming signal.

VII. IMPLEMENTATION

Our design of the intra-body communication channel is inspired by [33]. The authors of [33] are among the first to report reliable intra-body transmission based on capacitive coupling. Their designed receiver front-end achieves a transmission distance that spans the entire body. Our goal is to establish hand-to-hand transmission which typically reach around 180 cm for adults. We therefore adopted the impedance matching network proposed in [33] and followed the design choices found in Table I.

A. Measurement Setup

In order to simulate the pairing protocol between two devices, we designed a proof of concept for a body channel transmitter and receiver. For the purpose of our prototype setup, we did not implement two transceivers, but a separate transmitter and receiver. A more finished apparatus could combine the circuitry into two body channel transceivers that are capable of sending and receiving messages, i.e., bidirectional transmission.

The front-end of our receiver and transmitter implementation follow the exact same construction, which consists of two electrodes, the ground electrode and the touch-electrode. The person who pairs two devices only touches the touch-electrodes. The ground electrodes are floating. We describe the design of the electrodes in more detail in the following section.

We used lab measurement devices to implement the actual transmitter and receiver (see Figure 5). An arbitrary waveform generator acts as the transmitter and a software defined radio is the receiver. The waveform generator and the software defined radio are both controlled by a workstation computer that is used to specify the messages sent over the body channel and processes the signal received by the software defined radio. The receiver electrodes are directly connected to the software defined radio to record the incoming signal. The transmitter

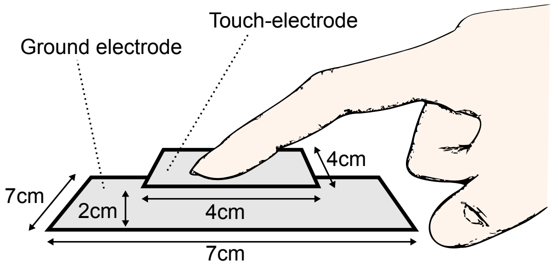

Fig. 6. Signal and ground electrodes are 2 cm apart and manufactured from two aluminum plates.

electrodes are connected to the waveform generator through an amplifier to boost the generated signal to the required 5 mW sending power.

For safety reasons and to minimize cross-talk, we made sure that the connections between the measurement devices are optically isolated. We also placed transmitter and receiver in such a way that they are separated by 150 cm and at least 200 cm away from any other electric conductor. Transmitter and receiver electrodes are also decoupled from earth ground or any other shared potential through a pair of Balun transformers. A Balun transformer converts a single-ended signal (a signal referenced to a known potential) to a balanced signal and thereby eliminates the effect of the shared potential by the grounded measurement instruments. This is absolutely necessary and simulates a realistic scenario for body channel communication, as otherwise the shared ground potential will form a direct return path, yielding an unrealistically strong signal. In a real scenario the transmitter and receiver are not in direct contact with each other and do not have a shared electric potential, such as earth ground. This is especially true if transmitter and receiver are implemented as battery-powered devices (e.g., in mobile devices).

B. Electrode Design

The touch-electrodes, i.e., the electrodes that interface the human body, we use are 4 cm by 4 cm sized aluminum plates with a thickness of 1 mm (see Figure 6). If the touch-electrodes are fabricated from a conductor, the effect of the electrode material on intra-body communication is marginal, see, e.g., [12]. In [4], aluminum and copper electrodes as well as pre-gelled electrodes, such as commercial AgCl electrodes used for electro-cardiogram measurements have been tested. Pre-gelled electrodes can have better performance than copper or aluminum plates for capacitive coupling as a body communication method, since the gel enhances conductivity and adherence to the skin. However, gelled electrodes are not an option for our proposed device pairing mechanism for both hygienic and usability reasons. We opted for aluminum plates, as our touch-electrodes should be reusable and a permanent feature of the device.

The ground electrodes of the transmitter and receiver normally do not need to be implemented specifically. In an actual device they would correspond to the ground plane of the circuit board of the transmitter or receiver. For our experiments, we implemented the ground electrodes as square aluminum sheets similar to the touch-electrodes. They measure 7 cm by 7 cm and thus cover an area of 49 cm^2 each. The required surface area of the ground electrodes for reliable body channel communication has been estimated in [9]. The authors of [9] developed a distributed RC model to simulate the characteristics of the human body channel when using capacitive coupling in the frequency range of 100 kHz to 150 MHz. According to the authors' empirical formula, 32 cm^2 is sufficient regardless of location of transmitter and receiver on the body if a bit error rate of 10^{-6} can be tolerated. Our ground electrodes cover 49 cm^2 and we achieve similar error rates (see Section VII-D).

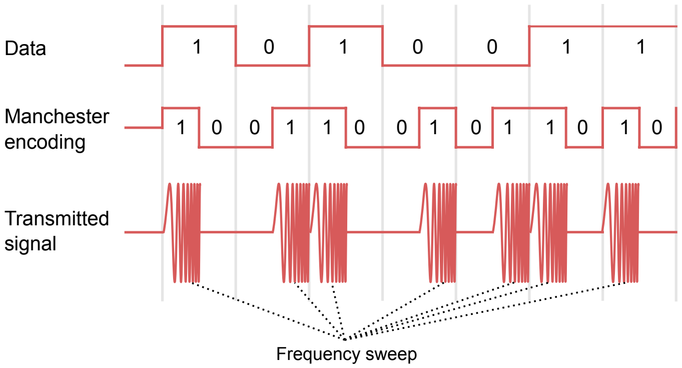

Fig. 7. Data is Manchester encoded. The transmitted signal follows an on-off-keying modulation. During the "on"-periods a frequency sweep is performed.

C. Data Encoding and Modulation

We apply Manchester coding to the data before it is sent over the body channel. The encoded messages are then transmitted using amplitude modulation in the form of on-off-keying. When the bit of the encoding is high, the power on the channel is "on" and similarly, if the bit of the encoding is low the power is "off". Our scheme differs from a simple on-off-keying in the way that we do not use a single carrier or center frequency for the "on"-period. Instead of transmitting on a single frequency, the sender performs a sweep over a range of frequencies (see Figure 7). The frequency sweep is not dependent on the transmitted data. Whenever the power is on the transmitter outputs a signal at a frequency of 0.5 MHz and keeps increasing the instantaneous frequency until it reaches 3.5 MHz and the power is turned off. The purpose of the frequency sweep is to characterize the communication channel. If the sweep is present in the transmitted signal, the receiver can measure the frequency-dependent attenuation over a broad spectrum and verify that the measured characteristics correspond to a human body channel.

D. Throughput and Error rate

With a duration of 1 milli-second per "on"-period, one data bit takes 2 milli-seconds to transmit. Assuming that there are no bit flips, this results in a theoretical data rate of 500 bits per second. For example, if the message authentication codes R_N and L_N from the pairing protocol have 56 bit length, just 224 milliseconds are required to transmit both MACs over the body channel.

In all our experiments, the measured bit error rate of the body channel for hand-to-hand transmission was below 10^{-6}. This means that under normal operating conditions, i.e., when

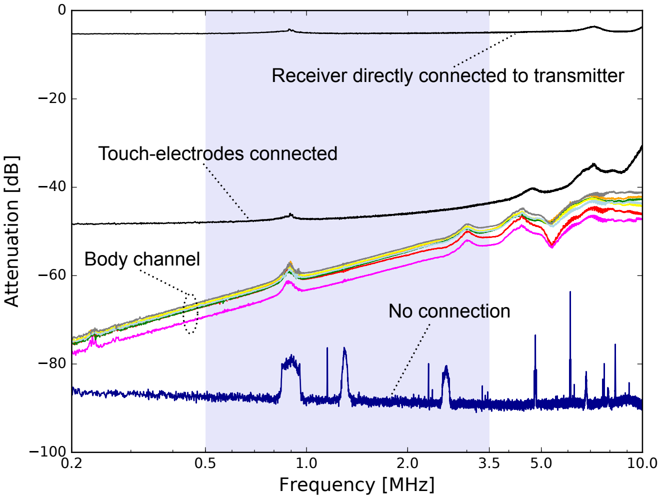

Fig. 8. Measured attenuation (S_{21} parameters) of the body communication channel. From top to bottom: Both electrodes of transmitter and receiver are directly connected to each other with a wire (first black line), only the touch-electrodes of transmitter and receiver are connected with a wire (second black line), transmitter and receiver communicate through a human body (colored lines for 7 different people), receiver and transmitter are not connected at all (dark blue line at bottom). The shaded area depicts the frequency range we use to distinguish the body channel.

the human body is not subjected to external interference, the probability for a flipped bit is very low. The transmission of two 56 bit message authentication codes is errorless with a probability of more than $(1 - 10^{-6})^{2 \cdot 56} = 99.98\%$ if the bit errors are equally likely to happen for every bit. Assuming the MACs have 56 bit length, it is therefore not necessary to compute error correcting codes and introduce redundancy into the messages that are sent over the body channel.

E. Body Channel Characteristics

Some of the energy transmitted on the body channel is lost due to the effect of the capacitive coupling and due to the fact that the human body is not a perfect conductor. As a consequence, the frequency sweeps that are sent by the transmitter are attenuated. In fact, the attenuation is frequency dependent, which means that not all parts of the frequency sweep are affected to the same extent. Provided the transmitter sends the sweeps at a fixed power level, the receiver can exploit this fact and measure the frequency dependent attenuation. Since there are no active elements in the body channel, the receiver essentially measures the S_{21} scattering parameter of the transmission line through the human body.

By extracting this information from the messages received through the touch-electrode, the receiver can characterize the communication channel. If the receiver knows the attenuation pattern that corresponds to a human body channel, it can verify if the received frequency sweeps have traveled through a human body by matching them with the known pattern.

In Figure 8, we show the channel characteristics for 7 different people when they are in physical contact with the touch-electrode of transmitter and receiver. We plot the attenuation over the frequency range from 0.2 MHz to 10 MHz and compare the body channel to the case where the touch-electrodes are either shorted-out or not connected at all. It is apparent that the human body channel exhibits characteristics different from other conductors, such as a cable for instance. If the touch electrodes are connected with each other through a copper wire, the attenuation is low throughout the entire frequency spectrum. Contrary to that, if the touch-electrodes of the transmitter and receiver are not connected at all, i.e., they are floating, we see that all the frequencies are completely attenuated and are not picked up by the receiver (bottom line in Figure 8).

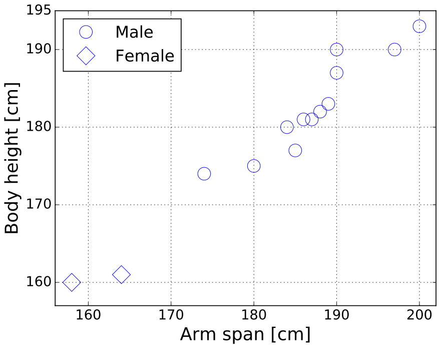

Fig. 9. Body dimensions of the study participants. Arm span is measured in a T-pose (fingertip to fingertip) and approximately represents the length of the body channel.

As explained earlier in Section II, capacitive coupling works in the frequency range of 1 MHz to 100 MHz. However, frequencies higher than 10 MHz are mostly surface waves [35]. We focus on the frequencies between 0.5 MHz and 3.5 MHz to extract the body channel characteristics. Figure 8 shows that the higher the frequency, the lower the attenuation, because more power is transmitted through the air. The signal does not travel through or along the human body any more and the channel characteristics become less unique to the human body (i.e., the human body acts as a high-pass filter). We capture the properties of the human body channel where they are most specific and can facilitate the distinction whether the characteristics belong to human body channel or not.

F. Experiment Dataset and User Safety

For the experimental analysis of our proposed pairing scheme, we collected data from a total of 15 study participants. The study was approved by the ethics board of the University of Oxford under the reference number R53956/001. The participant group of the study consisted of two women and 13 men who were between 22 to 45 years old. Figure 9 shows the body dimensions of the study participants. We collected more than 50 data transmissions per participant and conducted additional experiments to prove that our protocol is secure.

Our implementation of body communication is safe to use and does not pose a risk to human health. The return path for capacitive coupling goes through the air, which results in very high resistance and little current flow [34]. In fact, the current through the body never exceeded 12 micro-ampere (see Table I). This is much weaker than what commercially available body composition measurement devices emit. Body fat monitors, for instance, pass a current of up to 500 micro-amperes through a person [23].

In addition to the risk of current flow, we have to ensure that the exposure to the electromagnetic field created by the capacitive coupling does not jeopardize human health. We consulted the "Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields" issued by ICNIRP (see [1], [14]) and concluded that the electric field strength generated inside the human body stays well within the suggested limit of 1.35V/m per 1000 Hz.

Moreover, we verified that the power of our body channel transmitter does not violate FCC regulations [10]. We measured the strength of the radiated electromagnetic field with a rod antenna at a distance of 4 meters for a subset of our participant group. The electromagnetic waves radiated into the air did not exceed the limit of 30 μV/m in the entire frequency range we experimented in, i.e., from 0.2 MHz to 10.0 MHz.

Lastly, we made sure that our lab instruments are isolated from the touch-electrodes, such that even in the very unlikely event of a hardware failure the participants are not exposed to line voltage.

VIII. Experiments

In this section, we present experiments that document the properties of the body channel and validate the assumption that the body channel is read-only for an attacker that is not touching the body.

The read only property can be stated in two different ways and we validate both experimentally.

- We verify that a body channel enabled device can detect if a received message has been sent by another device that is physically connected to the same person or an outside signal source. The receiver should be able to classify messages according to their origin; if the message comes from a legitimate body channel or an external transmitter.
- We examine if it is possible to "inject" a message into the body channel in such a way that the physical properties of the message appear at the receiver as if the message was sent on the body channel.

We break the experiments down into these two statements and report the results in the following.

A. *Classification of Body Channel Messages*

Our proposed pairing protocol relies on the ability of the body channel receiver to distinguish messages based on their physical properties. This is important, not only from a security standpoint, but also with respect to usability. The device pairing protocol does not work if the receiver can not detect the body channel. To show that a body channel receiver can identify messages sent on body channel, we performed data transmission through the body channel of 15 test subjects under various conditions.

In order to capture data reflecting the intended use of the device pairing protocol, we asked the participants to touch receiver and transmitter electrodes as if they were paring two devices. With the collected data we establish a baseline of the attenuation pattern of the human body. We then analyze how the channel characteristics change when the body channel is modified, or if there is no human body present. We build and train a classifier that can exploit these differences and decide whether a previously unseen message has been sent on the body channel.

If the classifier is universal enough to distinguish between messages independently of the actual person involved in the pairing, it can be readily deployed in any body channel enabled device. Such a device would not require any user-specific input or enrolment to classify messages and therefore could be taken into operation without in-field adjustments or calibration.

a) Feature Extraction: The receiver captures the messages that are transmitted on the body channel in the form of the time varying voltage level at the touch-electrode. The measured electric signal is transformed to the frequency domain where the channel characteristics become apparent. We use the Fast Fourier Transform (FFT) to compute the frequency bins that correspond to the spectrum from 0.5 MHz to 3.5 MHz. The magnitudes of each bin constitute the feature values that are passed to the classifier for training. As an additional step, before we train the classifier, we normalize the extracted feature values to eliminate the effect the power of the transmitter has on classification.

b) Classifier: We use support vector machines (SVMs) to classify the channel characteristics and we treat the classification problem as supervised and binary. The classifier has to decide between two classes; the class of features that belong to the body channel and the class of all unwanted interactions with the body channel receiver (i.e., unwanted interactions are combined to one class for training).

c) Evaluation: We evaluate the classifier on samples that we gathered in multiple scenarios that each fall into one of those two classes. For the intended use of the body channel we tested two different settings. The participant is either standing or in a seated position when touching the electrodes.

The samples that represent unwanted interactions cover the following scenarios:

1) No connection between the transmitter and receiver electrodes. All electrodes are floating.
2) Transmitter and receiver electrodes are connected to each other through a wire.
3) Transmitter and receiver electrodes are facing each other at various distances (5 cm, 10 cm, 30 cm and 50 cm).
4) Transmitter is connected to either a rod antenna of 1 m length or a 25 cm by 80 cm aluminum sheet (a large surface area improves capacitive coupling) directly pointing at the receiver. This scenario represents an external transmitter communicating with the body channel receiver.
5) One of the participant's hand touches the electrode of the receiver, but his other hand is not in physical contact with the electrode of the transmitter. It hovers over the transmitter electrode at various distances (5 cm, 10 cm and 30 cm).
6) The participant only touches the receiver electrode. The transmitter is connected to a rod antenna or an aluminum sheet which is placed at a distance of 30

TABLE II. CLASSIFICATION RESULTS FOR BODY CHANNEL CHARACTERISTICS.

Wave Type	Accuracy	F1 score	AUC (ROC)
Sine wave	0.993 (± 0.018)	0.987 (± 0.033)	0.985 (± 0.037)
Square wave	0.943 (± 0.180)	0.918 (± 0.246)	0.988 (± 0.040)

Shown are the mean values of the metric and the 95% confidence interval.

cm and 60 cm from the participant. This scenario represents an external transmitter communicating with receiver while a person (accidentally) touches the receiver electrode.

The different scenarios listed above are repeated at different transmit power levels. We set the output voltage of the transmitter to 1, 2, 5 and 10 Volts. The data sent in these experiments consists of a random bit-string of 56 bit length.

All experiments are performed twice, once with a frequency sweep containing a sine wave and a second time with a square wave, to determine if the shape of the waveform plays a role in how the channel characteristics are elicited. Sine waves are a straightforward way to measure channel properties, but the study in [32] successfully applied short square pulses to intra-body communication using capacitive coupling. Since a frequency sweep with a square wave corresponds to a series of pulses of different duration, we also include square waves in our evaluation.

d) Results: We analyze a total of 1020 instances of the scenarios described above. They encompass data transmissions for every study participant in each of the outlined cases. The balance of the two classes, i.e., the ratio between the number of samples that represent the body channel and those that represent unwanted interactions is 1:1.

Table II shows the classification performance in terms of three metrics: accuracy, F1-score and the area under the ROC (receiver operating characteristic) curve. The results are obtained by running stratified 10-fold cross-validation. We observe that the SVM based classifier can detect the characteristics of the body channel with high accuracy. If a sine wave is used for the frequency sweep, the probability for a misclassification is less than 2%. All three different metrics are consistently high which suggests that the human body channel is very distinctive even when compared to the various other ways of interacting with the receiver. The results also show that the extracted characteristics are consistent across different people, regardless whether the study participants are sitting or standing. The body pose does not have a significant effect on the body channel. Figure 10 shows the receiver operating characteristic curve, representing body channel transmissions as positive samples and unwanted interactions as negative samples. Both curves are very close to each other, with "sitting only" slightly outperforming the other. The classifier can be tuned by setting the operation point to any point on the curve. Figure 10 shows that overall the classifier is conservative in assigning a new sample to the class of body channel characteristics and is more likely to reject it as an unwanted interaction.

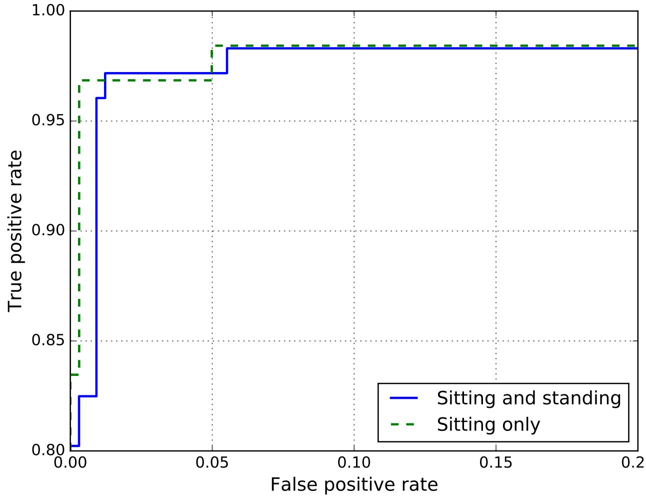

Fig. 10. Receiver operating characteristic (ROC) for the body channel classifier, zoomed into the upper left area. We compare the effect of two body poses: participants are sitting or standing when touching the electrodes (solid line) or sitting only (dashed line).

TABLE III. UNWANTED INTERACTIONS WITH THE BODY CHANNEL RECEIVER ACCORDING TO THEIR LIKELIHOOD FOR MISCLASSIFICATION IN [%]

Antenna Type	Participant touches receiver electrode	Receiver electrode is floating
Rod antenna		
at 30 cm	0.40	0.09
at 60 cm	0.01	0.00
Aluminum sheet		
at 30 cm	0.91	0.30
at 60 cm	0.09	0.00
Participant's hand hovers over transmitter electrode		
at 5 cm	70.1	N/A
at 10 cm	55.0	N/A
at 30 cm	1.20	N/A

Shown are mean values obtained by running 10-fold cross-validation.

If a square wave is used for the frequency sweep, the classifier does not perform as well as for a sine wave. The explanation for this behavior is the fact that a square wave generates more spectral components in the high frequency range. These frequencies are mostly transmitted through the air and therefore do not capture any of the distinctiveness of the human body channel.

In order to understand what scenarios exhibit channel characteristics that come closest to the actual body channel, we list the scenarios according to their likelihood for misclassification in Table III. We see that, if the participant is in contact with the touch-electrode of the receiver, but only hovers over the transmitter electrode, the channel characteristics are similar to the actual body channel. This is result is not surprising, because the additional distance between the body and the transmitter electrode will increase the capacitance of the channel, but not significantly change other physical properties of the channel. Capacitive coupling still works even if the body is not in direct contact with the emitter of the signal. If an external transmitter is used however, the channel characteristics only match an actual body channel to an extent. Table III shows that the rod antenna and the aluminum sheet are more successful in establishing a body channel if they are closer to receiver or the person. At a distance of more than 60 cm the chance of matching the body channel characteristics becomes negligible, assuming the transmitted signal corresponds to what the receiver expects, i.e., a frequency sweep from 0.5 MHz to 3.5 MHz. We investigate the case of an attacker changing the waveform for signal injection in the following section.

B. External Signal Injection

We have shown that the human body channel can be characterized on the basis of its frequency dependent attenuation pattern. We now approach the question if the body channel is read only from the perspective of the second statement: Can attacker transmit from an external source and by manipulating the signal, make it appear as if it was sent on the body channel?

To answer this question we make a number of observations. The first observation is that an attacker has two options, inject his own message on the body channel or modify another message. If he injects an entire message, he has to make sure that all frequency sweeps included in the message match the body channel characteristics. If the attacker's goal is to modify another message, he has to inject at least a part of a message. The messages on the body channel transmitter are Manchester coded and every bit of transmitted data consists of a period where power is on and off. Therefore, even to change a single bit, the attacker has to inject a signal that matches a frequency sweep emitted by a body channel transmitter. Regardless if the attacker injects an entire message or modifies another message, if the injection of a single sweep fails, then the message is automatically rejected by the classifier, because at least part of the signal has a different signature. We therefore focus on the injection of a single sweep signal in the following.

We also note that changing the overall transmit power does not help an attacker since a constant shift in the attenuation pattern (e.g., achieved by increasing the power of the transmitter) is removed during the normalization of the extracted features.

We divide signal injection attempts into the near and far field based on the attacker's distance to the body channel receiver. Near and far field define the behavior of the electromagnetic field around a receiving or transmitting antenna. In the far field "normal" electromagnetic radiation is dominant, whereas in the near field the electromagnetic field is mostly determined by non-radiative and quasi-static effects, such as capacitive coupling. For the purpose of our analysis, we define the boundary between near and far field to be where capacitive coupling becomes ineffective.

a) Far field: An attacker in the far field has to send a signal that matches the body channel signature like an attacker from the near field. However, an attacker in the far field can not rely on capacitive coupling because the electric field generated by electrostatic effects falls off with distance cubed [38]. The attacker has to resort to radio frequency transmission, but transmitting on the frequency band of 0.5 to 3.5 MHz at a power level such that the signal is picked up by the receiver electrode (or the human body, provided a person is touching the electrode) is not feasible. The electrodes as well as the person are by far from an optimal antenna for such low frequencies.

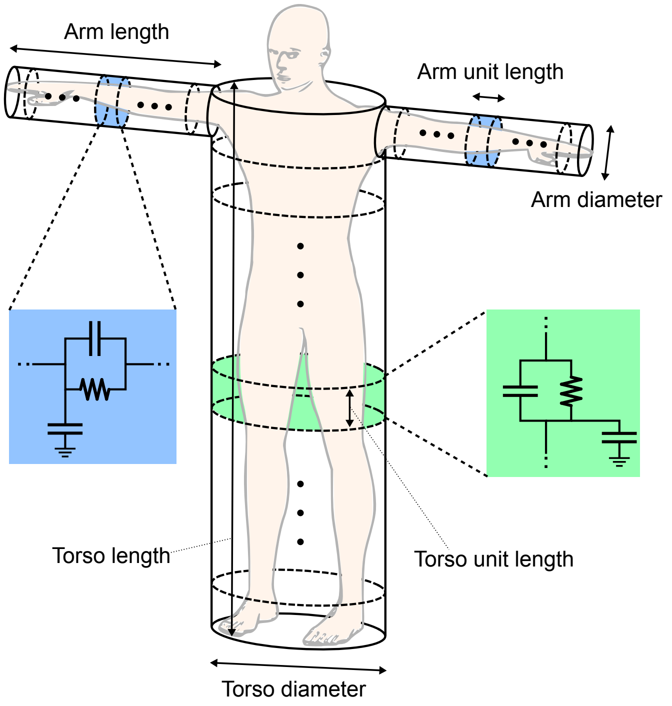

Fig. 11. Lumped network model for body channel. The human body is simplified to three connected cylinders. The cylinders are further divided into smaller units. Each unit can be modeled with a capacitor and a resistor in parallel, plus coupling capacitance to ground.

The human body does have an antenna effect because of its size [9], but at wavelengths on the order of 100 m it is not viable to induce a field strength at the receiver electrode that would result in a signal greater than thermal noise. Unless the transmitter is highly directional and has an output power in excess of 100 W, an attacker can not inject a meaningful signal, let alone a signal with a signature resembling the characteristics of the body channel. Aiming the antenna at the receiver further increases the complexity of an attack from the far field as well as signal propagation phenomenons such as multipathing that cause interference and fading.

b) Near field: Electrostatic coupling, such as capacitive coupling, has the highest chance of success for signal injection. Electrostatic effects diminish with the cube of the distance, but if an attacker is close enough to the receiver (or the person touching the receiver electrode), he can mitigate the attenuation by increasing the output power of his transmitter.

Capacitive coupling works by electrostatically coupling a current into the human body. The air gap between body and transmitter acts as a capacitor and the larger the gap, the higher its capacitance. A high capacitance results in a high-pass filter with a higher cut-off frequency and the lower frequencies are attenuated significantly.

The attacker can overcome this attenuation in two different ways: increase the output power at the transmitter and increase the surface area of the transmitter. This is congruent with the finding in Section VIII-A, where we show that the channel characteristics are more similar to the body channel when an aluminum sheet with a large surface area is connected to the transmitter instead of a rod antenna. Following this reasoning, an external transmitter needs to have high power, a large surface area and be placed close to the receiver.

c) Network Model for Body Channel: In order to understand if signal injections from the near field are feasible, we build a lumped network model for the body channel which is inspired by [9]. The model approximates the human body as three cylinders, one for the torso and two for each arm (see Figure 11). The cylinders are subdivided into units for which an approximation of the electric circuit can be given. Each unit can be modeled with a capacitor and a resistor in parallel, plus coupling capacitance to ground. The units for torso and arms have the same electric circuit, but different parameters. The length of a unit is 10 cm for both, arm and torso. The diameter of an arms is 10 cm and the diameter of the torso is 30 cm, respectively. Based on these dimensions, the values for capacitance and resistance per unit can be calculated from the dielectric properties of biological tissues [11].

Using this model the body channel transmitter and receiver can be attached anywhere on the human body, i.e., to any unit block of the model, and the resulting transmission characteristics can readily be computed. If we attach the transmitter to one hand and the receiver to the other hand, we obtain an accurate approximation of the body channel characteristics (see Figure 12).

To simulate an external transmitter that does not directly touch the body, we can attach the transmitter at multiple coherent blocks of the network model to take into account the distance to the body. The further away the transmitter is the larger the area that is affected by the capacitive coupling. In addition to that, and as mentioned above, the distance between transmitter and human body changes the air coupling capacitance between the transmitter and body which also needs to be simulated by the model.

In Figure 12 we simulate a large aluminum sheet (25 cm by 80 cm) aimed at the person from behind at a distance of 30 cm and compare it with actual measurements. We find that the model approximates the channel characteristics very well.

Figure 12 also shows that the channel characteristics for an external source, such as an aluminum sheet, look significantly different from the body channel. For an attacker to successfully inject a signal, he has to change the output power of his transmitter based on the currently transmitted frequency, e.g., in order to make the injection shown in Figure 12 match the body channel signature, the attacker has to constantly vary the power of the transmitter. For instance, between 0.5 MHz and 0.8 MHz he has to transmit at a lower power output, then increase the power and then back off, only to gradually increase the power again. We claim that this is not feasible due to two reasons.

- The attacker does not know the exact characteristics of the channel his transmitter creates and he can not measure them as this would require physical access.
- The attacker can try to precompute the channel characteristics, but this is likely to be inaccurate, since the attenuation pattern is very volatile.

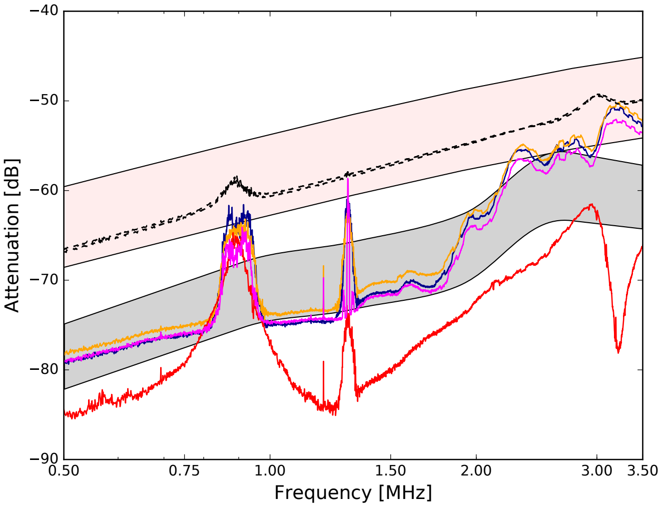

Fig. 12. Dotted lines represent attenuation patterns of the body channel obtained from two different people. Solid lines depict signal injections with an aluminum sheet. Bottom red line represents an attempt where the sheet is 5 cm further away from the body. Shaded areas show approximations using the lumped network model for a human with a body height between 140 and 180 cm.

In order to compute the channel properties, the adversary has to estimate the distance to the body as well as the location and size of the area on the body where capacitive coupling induces a current. Our experiments and the data simulated by the model demonstrate that the channel characteristics are very volatile and become increasingly difficult to approximate the further away the transmitter is placed. At around 30 cm distance, capacitive coupling becomes very weak and unpredictable. We give an example in Figure 12 that shows if the aluminum sheet is shifted by only 5 cm, the pattern looks significantly different. The bottom red line depicts an injection attempt when the sheet is placed at 35 cm instead of 30 cm distance from the person and the body channel receiver.

Together with the results from Section VIII-A, this insight lets us conclude that our stated read-only assumption for the body channel holds as long as there is a minimum distance of 50 cm between adversary's transmitter and the human body.

IX. Related Work

The idea of applying body channel communication to device pairing other than for medical sensors or implants has, to the best of our knowledge, not been documented so far. The paper that is most related to ours is [27] which proposes a body area network authentication scheme that does not depend on prior trust among the nodes. It is based on variations in received signal strength. Nodes that transmit on an on-body channel have a distinctive variation behavior of the signal strength. This behavior is different from a transmission on an off-body channel. The authors exploit this fact and perform clustering analysis to differentiate between an attacker and a legitimate node. This approach has similarities to our idea, as it also measures signal strength, but it exploits the physical movement of on-body sensors rather than capture the signal over a range of frequencies.

The study in [6] is related to our work as it proposes a method for robust key establishment among on-body sensors within a body area network using the human body channel. Key establishment is directly related to our problem statement, which is secure device pairing. However, their approach is different from ours, as the authors suggest to inject an artificial voltage signal below the action potential level of a human body to construct a covert communication channel. Their scheme uses electrical field propagation within the human body for communication that is secure against an outside eavesdropper.

Similar to the paper just mentioned, most research on the security of body channel communication and body area networks focuses on implantable and body-worn medical sensors. While our problem statement is substantially different from medical sensors and on-body devices, there are similarities. In particular the fact that the human body can serve as a transmission medium. Some on-body or implantable medical devices use body channel communication to transmit and receive sensor readings, either to and from each other or to establish communication with an external device which is used to monitor and program the implantable devices. An extensive survey and overview of literature about the security and privacy of body area networks and implantable medical devices can be found in [25].

We divide the remainder of the related work into (a) alternatives for secure device pairing and (b) applications of body communication published in literature outside system security.

a) Secure Device Pairing: Prior research has yielded a plethora of methods that implement secure device pairing. Most of them work by having the user authenticate information in an interactive way and augmenting the device pairing process with an out-of-band channel to mitigate MITM attacks. Various types of auxiliary channels have been proposed, e.g., the visual channel [22], the audio channel [31], or gesture-based channels [5], [21], [24]. Some approaches combine different out-of-bound channels, e.g., the proposal in [2] uses the the acoustic and vibration channel to reduce the risk of side-channel attacks. The authors mask the keying material that is transmitted via vibrations by actively injecting noise on the audio channel. Depending on the platform and the sensors available, many combinations of auxiliary channels are possible. In Augmented Reality headsets, for instance, it is feasible to combine the visual channel with a gesture-based channel, as suggested in [29].

We believe that, in terms of usability, gesture-based approaches such as [24] are most similar to the idea presented in this paper. The authors of [24] present a device pairing solution for smartphones where the user has to perform a hand gesture to point their phone into the direction of the target device. We consider such an approach comparable to touching two electrodes, which is required for our protocol to work. However, most gesture-based solutions need to explicitly capture and understand the user's intention signaled by their gesture. Therefore, the gesture needs to be sensed by the devices, often requiring another auxiliary channel for that purpose (e.g., the audio channel in case of [24]). Our solution on the other hand does not have to record any movements or gestures and has the advantage of only using one auxiliary channel — the human body.

Finally, a comparison and survey of a multitude of secure device pairing methods can be found in [16]. Worth mentioning is also the study in [15] that measures the influence user perception, security needs and other factors can have on device pairing method choices.

b) Applications of Body Channel Communication: The work most related to this paper in terms of application scenario is probably [20] which presents a system that allows a user to "wear" a unique key and unlock devices by simply touching them. The presented system consists of a wristwatch-like device that acts as a transmitter and houses a signal electrode. The electrode is in permanent contact with the user's skin around the wrist and emits data encoded in an electrical signal every time the user touches a receiver electrode with his finger. Via capacitive coupling, the data is transmitted to the receiver which might be embedded in a door, smart-phone or remote control device. Although such a novel unlocking mechanism bears a lot of potential with regard to usability, the paper draws no conclusions about the security of such system.

Also not in the field of security, but interesting to mention is the work in [28] which presents a near-field-sensing transceiver for intra-body communication between two or more devices as well as individuals themselves. The proposed transceiver features an electric-field sensor suitable for the fields generated by the human body when subjected to an electric signal. The authors' experiments include two transceivers communicating with each other through one and two human bodies.

X. Discussion

A. Body Position

Body position and body geometry can have an effect on the measurements as shown in Section VIII-A. We designed and conducted the experiments for two different body positions (seated and standing) to get an estimate of how much the attenuation of the received signal varies. The study in [19] found that for different test subjects the two positions, i.e., seated or standing, exhibited an attenuation of the same magnitude, which is in line with our results. The authors tested several other body poses and even body movement and reported that the attenuation changes by around 5 dB for a transmission distance of 120 cm. Hence, we conclude that body position has an insignificant impact on the use of capacitive coupling for our device pairing protocol.

XI. Conclusion

In this paper we proposed a novel approach to device pairing which builds upon the core idea of using intra-body communication. We presented a protocol that allows two devices to securely agree on a mutual secret by sending messages through the body of a person who is in physical contact with both devices. Incorporating the human body as a transmission medium entails a communication channel the devices can utilize to quickly and securely perform key confirmation, without the need for certificates or shared knowledge. Moreover, the human body channel provides the ability for the devices to extract physical properties that are very distinctive of this communication channel. We showed that these channel characteristics are sufficient to determine, with high probability, if a message has traveled from one device to the other via the body channel. Most importantly, however, our experiments document that the human body channel can not be interfered with from the outside as long as there is a distance of at least 50 cm between the external signal source and the person who is pairing the devices.

Considering the soaring number of electronic devices we use every day, the problem of bootstrapping secure communication between two unauthenticated devices will arise with increased frequency. We believe that our device pairing protocol is an attractive solution to this problem and enables even novice users to pair devices with a task that requires very little involvement other than the touch of two electrodes.

Finally, our paper leaves the interesting question for future work if intra-body communication could be used to enhance security in other protocols as well, such as in user authentication methods, for instance.

References

[1] A. Ahlbom, U. Bergqvist, J. Bernhardt, J. Cesarini, M. Grandolfo, M. Hietanen, A. Mckinlay, M. Repacholi, D. Sliney, J. A. Stolwijk *et al.*, "Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 ghz)," *Health physics*, vol. 74, no. 4, pp. 494–521, 1998.

[2] S. A. Anand and N. Saxena, "Vibreaker," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks - WiSec '16*. New York, New York, USA: ACM Press, 2016, pp. 103–108. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2939918.2939934

[3] J. Bae, H. Cho, K. Song, H. Lee, and H. J. Yoo, "The signal transmission mechanism on the surface of human body for body channel communication," *IEEE Transactions on Microwave Theory and Techniques*, vol. 60, no. 3, pp. 582–593, March 2012.

[4] M. A. Callejon, D. Naranjo-Hernandez, J. Reina-Tosina, and L. M. Roa, "A comprehensive study into intrabody communication measurements," *IEEE Transactions on Instrumentation and Measurement*, vol. 62, no. 9, pp. 2446–2455, 2013.

[5] C. Castelluccia and P. Mutaf, "Shake them up!: a movement-based pairing protocol for cpu-constrained devices," in *Proceedings of the 3rd international conference on Mobile systems, applications, and services*. ACM, 2005, pp. 51–64.

[6] S.-Y. Chang, Y.-C. Hu, H. Anderson, T. Fu, and E. Y. Huang, "Body area network security: Robust key establishment using human body channel." in *HealthSec*, 2012, pp. 5–5.

[7] X. M. Chen, P. U. Mak, S. H. Pun, Y. M. Gao, C.-T. Lam, M. I. Vai, and M. Du, "Study of channel characteristics for galvanic-type intrabody communication based on a transfer function from a quasi-static field model," *Sensors*, vol. 12, no. 12, pp. 16 433–16 450, 2012.

[8] N. Cho, L. Yan, J. Bae, and H. J. Yoo, "A 60 kb/s - 10 mb/s adaptive frequency hopping transceiver for interference-resilient body channel communication," *IEEE Journal of Solid-State Circuits*, vol. 44, no. 3, pp. 708–717, March 2009.

[9] N. Cho, J. Yoo, S.-J. Song, J. Lee, S. Jeon, and H.-J. Yoo, "The human body characteristics as a signal transmission medium for intrabody communication," *IEEE transactions on microwave theory and techniques*, vol. 55, no. 5, pp. 1080–1086, 2007.

[10] Federal Communications Commission. (2017) Electronic code of federal regulations: Title 47: Chapter I. [Online]. Available: http://www.ecfr.gov/cgi-bin/text-idx?mc=true&node=pt47.1.15

[11] S. Gabriel, R. Lau, and C. Gabriel, "The dielectric properties of biological tissues: Ii. measurements in the frequency range 10 hz to 20 ghz," *Physics in medicine and biology*, vol. 41, no. 11, p. 2251, 1996.

[12] K. Hachisuka, T. Takeda, Y. Terauchi, K. Sasaki, H. Hosaka, and K. Itao, "Intra-body data transmission for the personal area network," *Microsystem Technologies*, vol. 11, no. 8-10, pp. 1020–1027, 2005.

[13] C. H. Hyoung, J. B. Sung, J. H. Hwang, J. K. Kim, D. G. Park, and S. W. Kang, "A novel system for intrabody communication: touch-and-play," in *Circuits and Systems, 2006. ISCAS 2006. Proceedings. 2006 IEEE International Symposium on*. IEEE, 2006, pp. 4–pp.

[14] International Commission on Non-Ionizing Radiation Protection and others, "Guidelines for limiting exposure to time-varying electric and magnetic fields (1 hz to 100 khz)," *Health physics*, vol. 99, no. 6, pp. 818–836, 2010.

[15] I. Ion, M. Langheinrich, P. Kumaraguru, and S. Čapkun, "Influence of user perception, security needs, and social factors on device pairing method choices," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 2010, p. 6.

[16] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun, "A comparative study of secure device pairing methods," *Pervasive and Mobile Computing*, vol. 5, no. 6, pp. 734–749, 2009.

[17] K. S. Kwak, S. Ullah, and N. Ullah, "An overview of ieee 802.15.6 standard," in *2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)*, Nov 2010, pp. 1–6.

[18] Ž. Lucev, I. Krois, and M. Cifrek, "A capacitive intrabody communication channel from 100 khz to 100 mhz," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 12, pp. 3280–3289, 2012.

[19] Ž. Lučev, I. Krois, and M. Cifrek, "Effect of body positions and movements in a capacitive intrabody communication channel from 100 khz to 100 mhz," in *Instrumentation and Measurement Technology Conference (I2MTC), 2012 IEEE International*. IEEE, 2012, pp. 2791–2795.

[20] N. Matsushita, S. Tajima, Y. Ayatsuka, and J. Rekimoto, "Wearable key: Device for personalizing nearby environment," in *Wearable Computers, The Fourth International Symposium on*. IEEE, 2000, pp. 119–126.

[21] R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," *IEEE Transactions on Mobile Computing*, vol. 8, no. 6, pp. 792–806, 2009. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs{_}all.jsp?arnumber=4796201

[22] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human-verifiable authentication," in *Security and privacy, 2005 IEEE symposium on*. IEEE, 2005, pp. 110–124.

[23] OMRON Healthcare. (2017) Weight management - frequently asked questions. [Online]. Available: https://www.omron-healthcare.com/en-gb/products/weightmanagement

[24] C. Peng, G. Shen, Y. Zhang, and S. Lu, "Point&connect: intention-based device pairing for mobile phone users," in *Proceedings of the 7th international conference on Mobile systems, applications, and services*. ACM, 2009, pp. 137–150.

[25] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "Sok: Security and privacy in implantable medical devices and body area networks," in *Security and Privacy (SP), 2014 IEEE Symposium on*. IEEE, 2014, pp. 524–539.

[26] M. Seyedi, B. Kibret, D. T. Lai, and M. Faulkner, "A survey on intrabody communications for body area network applications," *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 8, pp. 2067–2079, 2013.

[27] L. Shi, M. Li, S. Yu, and J. Yuan, "Bana: body area network authentication exploiting channel characteristics," *IEEE Journal on selected Areas in Communications*, vol. 31, no. 9, pp. 1803–1816, 2013.

[28] M. Shinagawa, M. Fukumoto, K. Ochiai, and H. Kyuragi, "A near-field-sensing transceiver for intrabody communication based on the electrooptic effect," *IEEE Transactions on instrumentation and measurement*, vol. 53, no. 6, pp. 1533–1538, 2004.

[29] I. Sluganovic, M. Serbec, A. Derek, and I. Martinovic, "HoloPair: Securing Shared Augmented Reality Using Microsoft HoloLens," in *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)*, 2017, p. 13.

[30] Y. Song, Q. Hao, K. Zhang, M. Wang, Y. Chu, and B. Kang, "The simulation method of the galvanic coupling intrabody communication with different signal transmission paths," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 4, pp. 1257–1266, 2011.

[31] C. Soriente, G. Tsudik, and E. Uzun, "Hapadep: human-assisted pure audio device pairing," *Information Security*, pp. 385–400, 2008.

[32] Ž. L. Vasić, I. Krois, and M. Cifrek, "On a pulse response of a capacitive intrabody communication channel," in *EUROCON, 2013 IEEE*. IEEE, 2013, pp. 1785–1789.

[33] H. Wang, X. Tang, C. S. Choy, K. N. Leung, and K. P. Pun, "A 5.4-mw 180-cm transmission distance 2.5-mb/s advanced techniques-based novel intrabody communication receiver analog front end," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 12, pp. 2829–2841, 2015.

[34] H. Wang, J. Wang, and C. S. Choy, "A 2.5-mbps, 170-cm transmission distance intrabody communication receiver front end design and its synchronization technique research," in *Circuits and Systems (MWSCAS), 2014 IEEE 57th International Midwest Symposium on*. IEEE, 2014, pp. 643–646.

[35] J. Wang, Y. Nishikawa, and T. Shibata, "Analysis of on-body transmission mechanism and characteristic based on an electromagnetic field approach," *IEEE Transactions on Microwave Theory and Techniques*, vol. 57, no. 10, pp. 2464–2470, Oct 2009.

[36] M. S. Wegmueller, M. Oberle, N. Felber, N. Kuster, and W. Fichtner, "Galvanical coupling for data transmission through the human body," in *Instrumentation and Measurement Technology Conference, 2006. IMTC 2006. Proceedings of the IEEE*. IEEE, 2006, pp. 1686–1689.

[37] M. S. Wegmüller, "Intra-body communication for biomedical sensor networks," Ph.D. dissertation, ETH ZURICH, 2007.

[38] T. G. Zimmerman, "Personal area networks: Near-field intrabody communication," *IBM Systems Journal*, vol. 35, no. 3.4, pp. 609–617, 1996.