5-2014

ZEBRA: Zero-Effort Bilateral Recurring Authentication (Companion report)

Shrirang Mare
Dartmouth College

Andres Molina-Markham
Dartmouth College

Cory Cornelius
Intel Labs

Ronald Peterson
Dartmouth College

David Kotz
Dartmouth College

ZEBRA: Zero-Effort Bilateral Recurring Authentication (Companion report)

Dartmouth Computer Science Technical Report TR2014-748

Shrirang Mare[1], Andrés Molina-Markham[1], Cory Cornelius[2], Ronald Peterson[1], and David Kotz[1]

[1]*Institute for Security, Technology, and Society, Dartmouth College*
[2]*Intel Labs*

Abstract

We describe and evaluate Zero-Effort Bilateral Recurring Authentication (ZEBRA) in our paper that appears in IEEE Symposium on Security and Privacy, May 2014. In this report we provide a more detailed comparative evaluation of ZEBRA against other related authentication schemes. The abstract of the paper follows.

Common authentication methods based on passwords, tokens, or fingerprints perform one-time authentication and rely on users to log out from the computer terminal when they leave. Users often do not log out, however, which is a security risk. The most common solution, inactivity timeouts, inevitably fail security (too long a timeout) or usability (too short a timeout) goals. One solution is to authenticate users continuously while they are using the terminal and automatically log them out when they leave. Several solutions are based on user proximity, but these are not sufficient: they only confirm whether the user is nearby but not whether the user is actually using the terminal. Proposed solutions based on behavioral biometric authentication (e.g., keystroke dynamics) may not be reliable, as a recent study suggests.

To address this problem we propose ZEBRA. In ZEBRA, a user wears a bracelet (with a built-in accelerometer, gyroscope, and radio) on her dominant wrist. When the user interacts with a computer terminal, the bracelet records the wrist movement, processes it, and sends it to the terminal. The terminal compares the wrist movement with the inputs it receives from the user (via keyboard and mouse), and confirms the continued presence of the user only if they correlate. Because the bracelet is on the same hand that provides inputs to the terminal, the accelerometer and gyroscope data and input events received by the terminal should correlate because their source is the same – the user's hand movement. In our experiments ZEBRA performed continuous authentication with 85 % accuracy in verifying the correct user and identified all adversaries within 11 s. For a different threshold that trades security for usability, ZEBRA correctly verified 90 % of users and identified all adversaries within 50 s.

ZEBRA [10] is a token-based authentication scheme that authenticates users based on their interactions with the device. Unlike keystroke-based biometrics that authenticates users based *how* they type, ZEBRA authenticates users based on *what* interactions (e.g., typing, scrolling) they perform on the device and *when*. In ZEBRA users wear a wrist-bracelet (token) that has built-in accelerometer and gyroscope sensors and a short range wireless radio to communicate with the device. ZEBRA authenticates users by monitoring their hand movements, using the senors in the wrist-bracelet, when they are interacting with the device, and comparing the hand movements with the inputs received by the device during the interaction.

In ZEBRA the bracelet contains the identification information for its associated user, which it shares with the device to authenticate the user. The user can associate the bracelet with herself when she wears the bracelet, say by entering a PIN on the bracelet or through a secure channel to the bracelet. The bracelet clasp can detect when it is being taken off and it de-associates with the user when it is taken off.

This is a companion technical report for a paper to appear in the Proceedings of the IEEE Symposium on Security and Privacy, May 2014.

1 Comparison Framework

We compare ZEBRA with other related authentication schemes using the usability-deployability-security (UDS) evaluation framework [5]. The UDS framework defines a set of benefits to evaluate web authentication schemes, but many of those benefits are relevant to device authentication schemes. Table 1 summarizes our evaluation of ZEBRA and 7 other authentication schemes. We first define all the benefits and then present our comparative evaluation of ZEBRA and other related authentication schemes.

1.1 Benefits

The UDS framework defines total 25 benefits to evaluate web authentication schemes: 8 usability benefits, 6 deployability benefits, and 11 security benefits. We use total 15 benefits to evaluate ZEBRA and other related schemes: 12 benefits from the UDS framework and 3 additional benefits that are applicable to continuous authentication schemes.

As in the UDS framework, we rate each scheme as either offering or not offering the benefit of a property; if a scheme *almost* offers the benefit, but not quite, we indicate this with the *Quasi-* prefix.

1.1.1 Usability benefits

Benefits U1-U3 are from the UDS framework, so we briefly define them here; see Bonneau et al. [5] for details. Benefit U4 is also from the UDS framework but we slightly modify its definition and we explain the difference here. We introduce usability benefit U5 for continuous authentication schemes.

U1 *Memorywise-Effortless*: Users of the scheme do not have to remember any secrets at all.

U2 *Nothing-to-Carry*: Users do not need to carry an additional physical object to use the scheme. We grant a *Quasi-Nothing-to-Carry* if the scheme can be implemented on an object that users carry or wear everywhere all the time anyway, such as their mobile phone, wrist watch, wearable fitness devices.

U3 *Easy-Recovery-from-Loss*: A user can conveniently regain the ability to authenticate if the authentication credentials are forgotten or the token is lost. We grant a scheme *Quasi-Easy-Recovery-from-Loss* benefit if the user has to purchase a token but can reset the authentication credentials herself without having to involve another party. A user's authentication credential is the information that the user presents to the device to get authenticated, e.g., username and password, fingerprint. In this report we use refer authentication credentials as simply credentials, unless otherwise noted.

U4 *Physically-Effortless*: The authentication process does not require any physical user effort beyond what the user performs while interacting with the device to get his/her task done on the device. In other words, the scheme should be passive, i.e., it should not require any explicit input from the user, but the scheme can use the inputs the user anyway provides to the device to get his/her task done. A keystroke-based scheme that authenticates users based on their typing pattern is passive and considered to be physically effortless, but a voice-based scheme when the user does not use voice as input to the device is considered as requiring physical effort.

This definition is slightly different (stricter) from the UDS framework definition, which considers physically-effortlessness only for authentication and not continuous authentication, and hence in the UDS framework simple actions such as pressing a button are considered as effortless actions, but for a continuous authentication these actions do not remain physically effortless. We grant schemes *Quasi-Physically-Effortless* benefit if they require the user to perform an action which is easy and effortless to perform once.

U5 *No-Constraint-on-Using-the-Device*: The scheme should not add any constraint on how the user should use the device or interact with the device. We grant *Quasi-No-Constraint-on-Using-the-Device* benefit to schemes that add constraints that are easy to follow but do not require any additional physical effort from the user. For example, facial-recognition scheme requires the user to be in the camera's field of vision, which can be easy, but a voice-based scheme requires the user to provide audio input, which is easy but requires physical effort.

1.1.2 Deployability benefits

The following two deployability benefits are from UDS framework.

D1 *Accessible*: Users who can use passwords are not prevented from using the scheme by disabilities or other physical (not cognitive) conditions.

D2 *Negligible-Cost-per-User*: The total cost per user of the scheme, adding up the costs at the prover's end (any device/token required for the user to authenticate) and the cost at the verifier's end (any hardware and/or software required on the device to authenticate the user). *Quasi-Negligible-Cost-per-User* is awarded to the scheme if the required cost on prover's end can be masked with the devices users carry anyway and the verifying device already contains the required hardware.

1.1.3 Security benefits

Security benefits S1-S6 are from the UDS framework. We introduce two additional security benefits, S7 and S8, for continuous authentication schemes.

S1 *Resilient-to-Physical-Observation*: An attacker cannot impersonate a user after observing them authenticate one or more times. Attacks include shoulder surfing, filming the keyboard or mouse use [14], recording keystroke timings based on sensors near the keyboard [11], or thermal imaging the keypad [13].

S2 *Resilient-to-Internal-Observation*: An attacker cannot impersonate a user by intercepting the user's inputs from inside the user's device (e.g., by keylogging malware) or eavesdropping on the cleartext communication between the user's token (prover) and the authenticating device (verifier).

S3 *Resilient-to-Leaks-from-Other-Verifiers*: Nothing that a verifier could possibly leak can help an attacker impersonate the user to another device.

S4 *Resilient-to-Phishing*: An attacker who simulates the authentication process, e.g., by spoofing the authentication screen, cannot collect credentials that can later be used to impersonate the user on the actual device.

S5 *Resilient-to-Theft*: If the credentials are lost they cannot be used for authentication by another person who gains possession of it. The lost credentials can be passwords written down by paper or hardware tokens. This benefit penalizes single-factor schemes that do not offer any protection against theft.

This definition is slightly different than the UDS definition. In the UDS framework this benefit is considered only for schemes in which physical objects are used for authentication; we consider theft of even non-physical credentials such as passwords, which can be stolen when people write them down. As in the UDS framework, we grant *Quasi-Resilient-to-Theft* if the scheme protects the credential with the modest strength of a PIN.

S6 *Require-Consent*: The user is authenticated only with the user's consent or intent. The UDS benefit requires an 'explicit' consent, which can make a continuous authentication scheme unusable, so we remove the 'explicit' consent requirement and require the scheme to use a passive consent or intent that matches users' mental model, i.e., users should not be authenticated when they are not using the device.

We grant *Quasi-Require-Consent* benefit to schemes that are better than consent by proximity alone, i.e., authenticating a user if she is in radio proximity of the device, but do not require a user to interact with the device to express intent to use the device. For example, facial-recognition based or voice-based authentication schemes may wrongly assume the user's intent to use a device if she is present in front of the device's camera or speaking near the device, even though she may not be using the device. Whereas a keystroke-based scheme authenticates a user when she is typing (i.e., using) the device, so these schemes are labeled *Require-Consent*. While evaluating this benefit we do not consider impersonation attacks by an adversary.

S7 *Verify-Actual-User*: The scheme can verify whether the user is actually using the device at any point in time. This benefit penalizes schemes one-time authentication schemes, which do not verify the user after the user

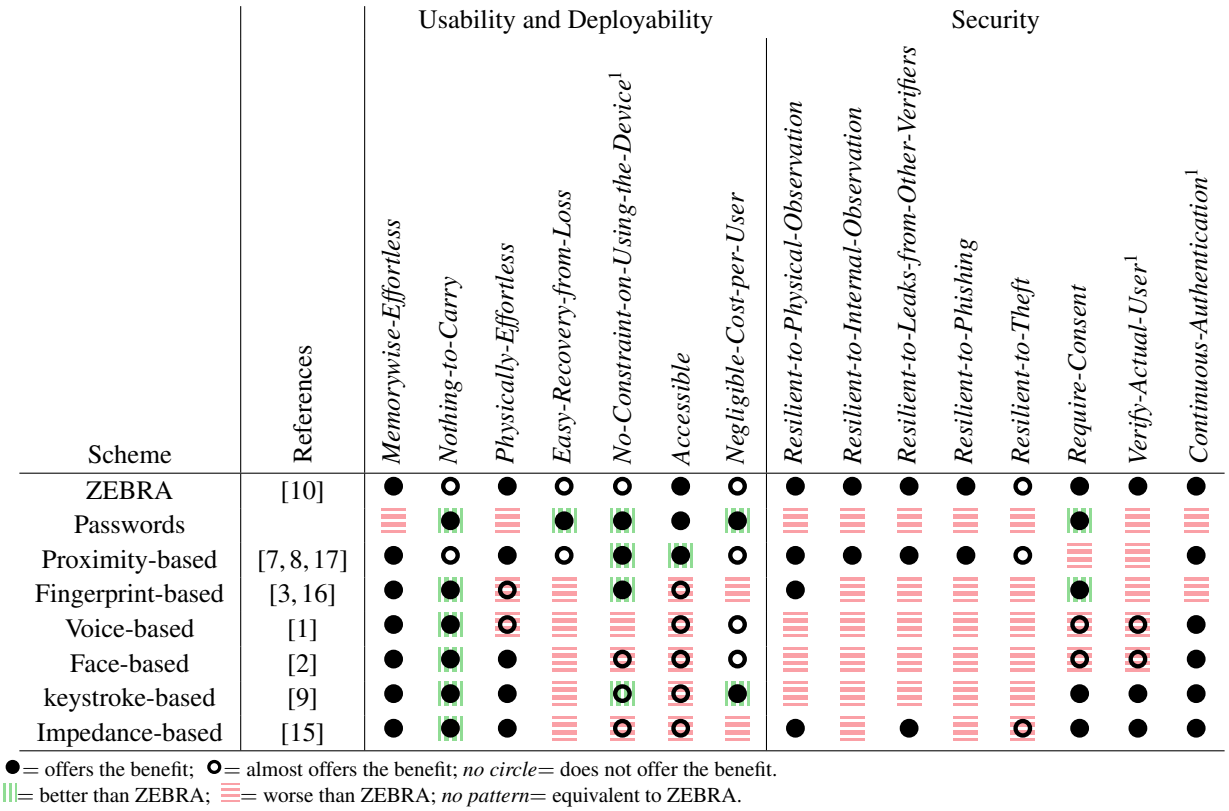
authenticates once. We grant *Quasi-Verify-Actual-User* benefit to schemes that do weak verifications, such as verifying whether the user is in front of the device (face-based schemes) or whether the user is speaking to the device (voice-based).

S8 *Continuous-Authentication*: The scheme should continuously authenticate the user while she uses the device.

2 Comparative Evaluation

Now we compare several candidates for continuous authentication, using the above framework.

Table 1: Comparative evaluation of ZEBRA against other authentication schemes.



[1] Additional properties, not in UDS framework.

2.1 ZEBRA

ZEBRA is *Memorywise-Effortless* and *Physically-Effortless* as users do not have to memorize any secret or take any explicit action to authenticate. ZEBRA provides *Quasi-Nothing-to-Carry* benefit as it can be integrated with their smart-watch or wrist fitness device It provides *Quasi-Easy-Recovery-from-Loss* as the user can easily replace her bracelet by purchasing a new one. It is *Accessible* as users who can type can use this scheme and we rate it as *Quasi-Negligible-Cost-per-User* because it can be integrated with existing fitness wrist-devices that users are increasingly wearing everyday. ZEBRA provides *Quasi-No-Constraint-on-Using-the-Device* as it requires a user to use the bracelet hand to provide inputs, but otherwise it adds no constraints on device usage. ZEBRA is *Resilient-to-Physical-Observation*,

Resilient-to-Internal-Observation, *Resilient-to-Leaks-from-Other-Verifiers*, and *Resilient-to-Phishing* as it does not use any stored secret for authentication.

We grant ZEBRA *Quasi-Resilient-to-Theft* because it can be made resilient to theft either by using a special clasp that deassociates the bracelet with the user when it is taken off and once deassociated the bracelet cannot be used to authenticate as that user, or by using a biometric that identifies the bracelet wearer [6]. ZEBRA does *Require-Consent* as it authenticates only when a user is providing inputs to the device, i.e., when the user is using the device. ZEBRA does *Verify-Actual-User* as it verifies the user who is interacting with it, and it does *Continuous-Authentication*.

2.2 Passwords

Passwords clearly are not *Memorywise-Effortless*. They provide *Nothing-to-Carry* benefit, but they are not *Physically-Effortless* as passwords need to be typed, but they do provide *Easy-Recovery-from-Loss* as they can be easily reset. They are *Accessible* because we defined this benefit with respect to them. They have *Negligible-Cost-per-User* and they add *No-Constraint-on-Using-the-Device* once the user authenticates by entering the right password, because they are one-time authentication schemes.

Passwords are not *Resilient-to-Physical-Observation* as they can be easily recovered by a video of keyboard or by carefully observing the user type the password [4] or using a sensor near the keyboard [11]. They are not *Resilient-to-Internal-Observation* as keylogging malware can easily capture the entered password. They are also not *Resilient-to-Leaks-from-Other-Verifiers* if the user uses the same password. They are not *Resilient-to-Phishing* or *Resilient-to-Theft* as the attacker can use the obtained password to impersonate the user. They do *Require-Consent* as the users have to enter their passwords to authenticate. Passwords do not *Verify-Actual-User* because the device assumes the current user is the user who last authenticated and they do not provide *Continuous-Authentication*.

2.3 Proximity-based schemes

Proximity-based schemes authenticate users if they are in the proximity of the device as determined by the wireless radio signal strength from a token they carry. These schemes are *Memorywise-Effortless* and *Physically-Effortless*, and *Quasi-Nothing-to-Carry* as users have to carry the proximity tokens, but these tokens can be integrated with their smartphones. They are not as easy to recover as passwords but they can be recovered by buying another token, so we grant them *Quasi-Easy-Recovery-from-Loss*. They are *Accessible* and better than ZEBRA because it works even for users who are passively using a device (i.e., not typing) or users who are not typing with the bracelet hand (e.g., one hand typing). The wireless token can be integrated with any electronic jewelry the user wears or the user's phone so we grant *Quasi-Negligible-Cost-per-User*, and these schemes add *No-Constraint-on-Using-the-Device*.

These schemes are *Resilient-to-Physical-Observation*, *Resilient-to-Internal-Observation*, *Resilient-to-Leaks-from-Other-Verifiers*, and *Resilient-to-Phishing* if we assume that the communication between the token and the device is secure and cannot be eavesdropped by the attacker. These schemes can be somewhat resilient to theft by using a special clasp that deassociates with the user when it is taken off, and once deassociated it cannot be used to authenticate as that user. So we grant these schemes *Quasi-Resilient-to-Theft* because they can be made resilient to theft by ensuring that they cannot be used to impersonate a user when they are not being worn by that user. These schemes do not *Require-Consent* as the user is authenticated whenever she is in the proximity of the device, without any consent, and for the same reason these schemes do not *Verify-Actual-User*. They do provide *Continuous-Authentication*, but they may not authenticate the user who is actually using the device and we reflect this by not granting them the *Verify-Actual-User* benefit.

2.4 Fingerprint-based schemes

Fingerprint-based schemes are *Memorywise-Effortless* and *Nothing-to-Carry*, as in any biometric scheme, but they are not *Physically-Effortless* as the user has to swipe or hold the finger on the reader. They do not provide *Easy-Recovery-from-Loss* as a fingerprint, once stolen, cannot be reset. We grant them *Quasi-Accessible* because they are not effective against users who do not have fingerprints or if the user's fingerprint changes due to external factors, such as an injury. They do not provide *Negligible-Cost-per-User* because each device needs have a fingerprint scanner. They add

No-Constraint-on-Using-the-Device because, like passwords, they are one-time authentication and once authenticate they allow full access to the user until she logs out.

They are *Resilient-to-Physical-Observation* as they are hard to capture by video but they are not *Resilient-to-Internal-Observation*, *Resilient-to-Leaks-from-Other-Verifiers*, *Resilient-to-Phishing*, and *Resilient-to-Theft*. Users have to swipe their finger to get authenticated so they do *Require-Consent* but they do not *Verify-Actual-User* because like passwords they assume the current user is the same user who last authenticated, and they do not provide *Continuous-Authentication*.

2.5 Voice-based schemes

Voice-based authentication schemes are physiological biometric schemes that authenticate users based on their unique voice patterns. Voice-based authentication can be used for initial authentication, as for passwords or fingerprints, with many of the same properties as fingerprints. Voice-based methods can also be used for continuous authentication, which is how we evaluate them here.

These schemes are also *Memorywise-Effortless* and *Nothing-to-Carry* but they are not *Physically-Effortless* as the user has to speak out loud for authentication and they do not provide *Easy-Recovery-from-Loss*, like other biometrics. We grant them *Quasi-Accessible* because some these schemes do not work for speech-impaired users or if the user's voice changes due to illness or injury. We consider them *Quasi-Negligible-Cost-per-User* because many devices today have a built-in microphone and it is inexpensive to add one, if required. To perform continuous authentication with these schemes users need to speak out loud frequently so they do not provide *No-Constraint-on-Using-the-Device* benefit.

They are not *Resilient-to-Physical-Observation* as an adversary can easily record a user's voice with a microphone. These schemes are also not *Resilient-to-Internal-Observation*, *Resilient-to-Leaks-from-Other-Verifiers* and *Resilient-to-Phishing*, and once the voice credentials are stolen an adversary can use them to impersonate the user so these schemes are not *Resilient-to-Theft*. Users have speak out loud to authenticate, so we grant these schemes *Quas-Require-Consent*. We grant these schemes *Quasi-Verify-Actual-User* because these schemes verify whether the user is speaking near the device and not whether the user is actually using the device. These schemes can be used to perform *Continuous-Authentication*.

2.6 Face-based schemes

Face-based schemes authenticate a user based on the device's recognition of the image of her face as captured by the device's camera. Face-based authentication can be used for initial authentication, as for passwords or fingerprints, with many of the same properties as passwords. Face-based methods can also be used for continuous authentication, which is how we evaluate them here.

These schemes are *Memorywise-Effortless* and *Nothing-to-Carry*, like any biometric, and these schemes are also *Physically-Effortless* as the user simply has to be in-front of the camera when using the device. These schemes, like voice and fingerprint biometrics, do not provide *Easy-Recovery-from-Loss*. We grant them *Quasi-Accessible* because these schemes may not perform with wearables (e.g., glasses), in poor lighting, or if the user's face changes due to an injury. These schemes provide *Quasi-Negligible-Cost-per-User* because many devices today have a built-in video camera and it is inexpensive to buy a camera, if required. We grant these schemes *Quasi-No-Constraint-on-Using-the-Device* because they require the user to be present in the camera's field of view.

These schemes are not *Resilient-to-Physical-Observation* as an adversary can easily capture as image of the user's face with a camera. These schemes are also not *Resilient-to-Internal-Observation*, *Resilient-to-Leaks-from-Other-Verifiers* and *Resilient-to-Phishing*, and *Resilient-to-Theft*. We grant these schemes *Quasi-Require-Consent* because they require the user to be within the camera's field of vision, which is a better indication of intent to use a device than simply being in proximity of the device. These schemes do not *Verify-Actual-User* as the user who is camera's field of view may not be the one who is actually using the device, but they can provide *Continuous-Authentication*.

2.7 Keystroke-based schemes

Keystroke-based schemes authenticate users based on their typing behavior, which is measured using keystroke-dynamics that includes properties such as the time between two keystrokes or the time for each keystroke. These schemes are based on our behavior and hence are *Memorywise-Effortless* and *Nothing-to-Carry*. Although these

schemes require typing, we grant them *Physically-Effortless* because these schemes can be designed to use the typing inputs that the user provides to the device and do not require any explicit input from the user. These schemes, like some other biometric schemes, do not provide *Easy-Recovery-from-Loss* and we grant them *Quasi-Accessible* because they will not work if the user's typing behavior changes due to the user's mood, stress, different type of devices, or some injury.

These schemes have *Negligible-Cost-per-User* as there is not additional hardware cost. There is the initial training cost for each user, and maybe for each device, but we consider that cost negligible. Other than the constraint that users should type, which users anyway do to interact with most devices, these schemes do not add any other constraint so we grant them *Quasi-No-Constraint-on-Using-the-Device* and rate them better than ZEBRA because ZEBRA adds an additional small constraint that the user has type with both hands or the bracelet hand, i.e., the user should use the bracelet hand during typing. sub These schemes are not *Resilient-to-Physical-Observation* as the keystroke dynamics can be recorded using a sensor near the keyboard [11]. They are also not *Resilient-to-Internal-Observation*, *Resilient-to-Leaks-from-Other-Verifiers* and *Resilient-to-Phishing*. These schemes are not *Resilient-to-Theft* because, once the keystroke dynamics of a user are stolen, an adversary can use them to impersonate the user [12]. As the user has to type in order to be authenticated and typing indicates the intent to use a device, these schemes *Require-Consent* to authenticate. These schemes *Verify-Actual-User* as they authenticate the user who is providing keyboard input to a device, i.e., who is actually using the device, and hence they can provide *Continuous-Authentication*.

2.8 Impedance-based schemes

These schemes authenticate a user based on her body's impedance response to small electric current passed through her body [6, 15]. For continuous authentication on a device Rasmussen et al. [15] proposed instrumenting the keyboard of the device and measure the body's impedance response when an electric current is passed through one hand and received through another when the user is typing.

Like other biometric scheme, these schemes are *Memorywise-Effortless* and *Nothing-to-Carry*. We consider these schemes *Physically-Effortless* because these schemes can authenticate when the user is using the device (i.e., typing) without requiring the user to provide any explicit input. These schemes do not provide *Easy-Recovery-from-Loss*. We grant them *Quasi-Accessible* because human body's impedance response can change due to external environmental factors such as temperature or water intake of the user. As these schemes require instrumenting keyboards and the required additional hardware is not inexpensive, these schemes require more than *Negligible-Cost-per-User*. These schemes place an additional constraint that the user should use keep both hands in contact with the keyboard when typing, so we grant them *Quasi-No-Constraint-on-Using-the-Device* and rate them worse than ZEBRA.

These schemes are *Resilient-to-Physical-Observation* but they are not *Resilient-to-Internal-Observation* and *Resilient-to-Phishing*. They schemes can be made *Resilient-to-Leaks-from-Other-Verifiers* by using a different frequency-dependent response for each device so that a credential leaked from a device cannot be used to authenticate on another device. Although an adversary can use the stolen credentials to impersonate the user on the device, these schemes can prevent the adversary from using the credentials for one device on another, so we grant these schemes *Quasi-Resilient-to-Theft*. As typing indicates intent to use a device, these schemes *Require-Consent* and they *Verify-Actual-User* and can provide *Continuous-Authentication*.

3 Summary

In this report we present a framework to evaluate continuous authentication schemes and we do a comparative evaluation of ZEBRA with 7 other authentication schemes. As per our evaluation (Table 1) ZEBRA is a secure, usable, and deployable continuous authentication scheme: ZEBRA rates highest (with most solid circles) compared to the other 7 authentication schemes for the security properties that we considered; Password-based schemes are most deployable compared to all schemes, but among continuous authentication schemes ZEBRA and Proximity-based schemes are most deployable schemes; and in usability, ZEBRA is equally or more usable than other authentication schemes.

Acknowledgements

We thank Joseph Bonneau for sharing the figures in Table 1. This research results from a research program at the Institute for Security, Technology, and Society at Dartmouth College, supported by the National Science Foundation (Secure and Trustworthy Computing Program) under award number 1329686, and by the Department of Health and Human Services (SHARP program) under award number 90TR0003-01. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors.

References

[1] P. Aleksic and A. Katsaggelos. Audio-visual biometrics. *Proceedings of the IEEE*, 94(11):2025–2044, Nov 2006. DOI 10.1109/JPROC.2006.886017.

[2] Face Unlock On Android 4.0. Online at http://www.huffingtonpost.com/2011/10/19/face-unlock-ice-cream-sandwich_n_1020207.html.

[3] Apple iPhone 5S. Online at http://www.apple.com/iphone-5s.

[4] D. Balzarotti, M. Cova, and G. Vigna. Clearshot: Eavesdropping on keyboard input from video. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, pages 170–183, May 2008. DOI 10.1109/SP.2008.28.

[5] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, pages 553–567, May 2012. DOI 10.1109/SP.2012.44.

[6] C. Cornelius, R. Peterson, J. Skinner, R. J. Halter, and D. Kotz. A wearable system that knows who wears it. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*, June 2014. Accepted for publication, DOI 10.1145/2594368.2594369.

[7] M. D. Corner and B. D. Noble. Protecting applications with transient authentication. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 57–70. ACM, 2003. DOI 10.1145/1066116.1066117.

[8] C. E. Landwehr. Protecting unattended computers without software. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, pages 274–285. IEEE Computer Society, 1997. Online at http://dl.acm.org/citation.cfm?id=872015.872112.

[9] S. Lima e Silva Filho and M. Roisenberg. Continuous authentication by keystroke dynamics using committee machines. In S. Mehrotra, D. Zeng, H. Chen, B. Thuraisingham, and F.-Y. Wang, editors, *Intelligence and Security Informatics*, volume 3975 of *Lecture Notes in Computer Science*, pages 686–687. Springer Berlin Heidelberg, 2006. DOI 10.1007/11760146_90.

[10] S. Mare, A. Molina-Markham, C. Cornelius, R. Peterson, and D. Kotz. ZEBRA: Zero-effort bilateral recurring authentication. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, May 2014. DOI 10.1109/SP.2014.51.

[11] P. Marquardt, A. Verma, H. Carter, and P. Traynor. (sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 551–562. ACM, Oct. 2011. DOI 10.1145/2046707.2046771.

[12] T. C. Meng, P. Gupta, and D. Gao. I can be you: Questioning the use of keystroke dynamics as biometrics. In *Proceedings of the Network and Distributed Systems Security Symposium (NDSS)*, 2013. Online at http://flyer.sis.smu.edu.sg/ndss13-tey.pdf.

[13] K. Mowery, S. Meiklejohn, and S. Savage. Heat of the moment: Characterizing the efficacy of thermal camera-based attacks. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2011. Online at http://www.usenix.org/events/woot11/tech/final_files/Mowery.pdf.

[14] R. Raguram, A. M. White, D. Goswami, F. Monrose, and J.-M. Frahm. iSpy: automatic reconstruction of typed input from compromising reflections. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, CCS '11, pages 527–536. ACM, 2011. DOI 10.1145/2046707.2046769.

[15] K. B. Rasmussen, M. Roeschlin, I. Martinovic, and G. Tsudik. Authentication using pulse-response biometrics. In *Proceedings of the Network and Distributed Systems Security Symposium (NDSS)*, 2014. Online at http://www.internetsociety.org/sites/default/files/08_1_0.pdf.

[16] A. Ross, J. Shah, and A. Jain. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):544–560, April 2007. DOI 10.1109/TPAMI.2007.1018.

[17] F. Stajano. Pico: No more passwords! In B. Christianson, B. Crispo, J. Malcolm, and F. Stajano, editors, *Security Protocols XIX*, volume 7114 of *Lecture Notes in Computer Science*, pages 49–81. Springer-Verlag Berlin, Mar. 2011. DOI 10.1007/978-3-642-25867-1_6.