Connection Resilient Bodycam with Built-In Non-Repudiation and Verification Features

Mattias Duffy, Rahma Moalin Mohamed and Prayatna Timalsina

April 22, 2020

Connection Resilient Bodycam with Built-In Non-Repudiation and Verification Features

Duffy
Cybersecurity dept. Volgenau School
George Mason University
Fairfax, US
mduffy8@gmu.edu

Moalin-Mohamed
Cybersecurity dept. Volgenau School
George Mason University
Fairfax, US
rmoalinm@gmu.edu

Timalsina
Cybersecurity dept. Volgenau School
George Mason University
Fairfax, US
ptimalsi@gmu.edu

***Abstract*—Police Body-worn cameras (BWCs) have been an important addition to the police toolkit and have been shown to resolve cases faster, reduce paperwork, and make citizens feel safer. Despite these benefits, body camera technology is quite outdated as an officer still chooses what to record and what to submit for evidence. Only one copy of the footage exists, with the officer choosing what to record and what to submit for evidence. This evidence could either be destroyed before submission by an attacker or not recorded in the first place by a negligent officer. In order to ensure validity, integrity of video and provide non-repudiation of an officer's actions, we propose a solution that provides these services just by using a smart phone.**

***Index Terms*—Body Worn Cameras (BWCs), Non-Repudiation, Identity Verification, Identity Validation, Cell Phones**

I. Introduction

In the past decade, use of Body-worn cameras (BWCs) in Law Enforcement agencies has catapulted in popularity. In 2013, almost a third of agencies used video cameras on patrol officers [1, pp. 94]. Just 3 years later, 60% of local police departments and 49% of sheriffs' offices had fully deployed BWCs in their organizations. A main cause for this rapid adoption, was the social backlash seen in high profile cases such as the shooting of Trevon Martin in 2012, the shooting of Michael Brown by a Ferguson in 2014 and the others. In almost every case, video was used as a key piece of evidence to corroborate eye witness' accounts. As a result, BWCs was seen as a way to increase accountability and transparency for police and law enforcement [2] [1].

While BWCs have many supposed benefits such as *better transparency, increased civility, quick resolution of complaints, corroborating of other evidence, and training opportunities*, not all claims are positive. Other parties claim that they could lead to *de-policing and increased prosecutions* [3]. In the landmark survey by the Center for Evidence-Based Crime Policy at George Mason University, researchers looked through a body of 70 empirical studies to understand what effects BWCs really had on officer-citizen behaviors and relationships.

What the survey found was that while there were some concrete positive effects, the implementation of BWCs had a large impact on results. More research must be done on how BWC affect Officer-Citizen relationships and police organizations themselves.

The reason why such a gap exists may be because the push came from the people up to the police departments, many BWC solutions were implemented with out proper research or design considerations [1, pp. 95]. This can be seen as departments adopting the technology of the time vs designing the technology and operating procedures that fit department needs. A clear example if this, is the state of security in body cameras.

According to the Office of Justice Programs, it was estimated that about 47 percent of the 15,328 Law Enforcement agencies in the United States had deployed body cameras [4]. Although the addition of body cameras on law enforcement officers' and their cars has added much benefit of providing evidence, it also has created vulnerability for those evidence to be tampered by the very law enforcement officers before reaching the court. In this paper, we outline some areas where security can be improved and demonstrate a solution that we believe better fits law enforcement needs for a lower cost.

II. Current State of BWCs

In 2018, security researcher, Josh Mitchell looked at 5 body cameras from 6 different body camera brands. The companies Vievu, Patrol Eyes, Fire Cam, Digital Ally, and CeeSc market their products specifically to Law Enforcement agencies all around the world. In all but one of these cameras, there are vulnerabilities that allowed an attacker to modify or delete media, leaving no indication of changes. While there were numerous flaws and vulnerabilities found in each device due to poor implementation, Mitchell also identified some industry wide security issues [5].

There were also no checks on devices that the footage submitted for evidence was intact or from an authenticated user [5]. 4 out of 5 BWCs had WiFi Radios that broadcast information allowing an attacker to know the make, model, and identifying code device. None of the tested devices had signed firmware so an attacker could easily infect devices with malicious code. The categories of flaws are as follows.

A. Industry-Wide Flaws

- No Digital Signatures
  A digital signature is an encrypted hash of data that you are sharing with another party. With a digital signature, you ensure that the message came from a specific sender (*authenticity*) and has not been changed in transit (*integrity*) [6]. In addition to these services, digital signatures also provide *Identity Verification, Validation, and Non-Repudiation*. Because footage can be tampered with and altered in subtle ways (especially with new deep fake AI algorithms), it is possible for realistic but false videos to be circulated as evidence. Therefore, it is necessary to prove that the video is associated with a real identity, and that the video is associated with the correct identity. Since the users identity is validated and verified, it is possible to prove that they took a certain action [7].

- Identifiable Data
  If there is information broadcast from the device that identifies it as a police device such as MAC address or SSID, it can give attackers the ability to track or target these devices for attack. [5].

- Un-signed Firmware
  Without checks to make sure that firmware is authentic, an attacker can upload arbitrary code onto the device. This is perhaps the most dangerous flaw because it allows the attacker to perform the widest range of attacks.

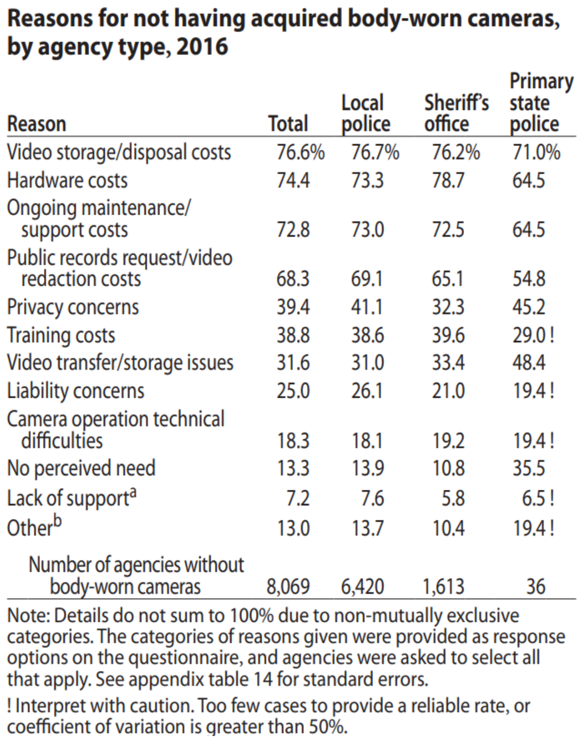
Since 2018, much has changed in the BWC world. The largest BWC supplier Axon is creating cameras that seem to be more secure and specialized for law enforcement needs. According to their website, updates are retrieved, installed, and validated during the normal device charging and data transfer process so its assumed that firmware signed and controlled carefully. In addition, based on their claims about ensuring video validity and authenticity, they are using digital signatures to sign video evidence. While it is clear that they have security in mind when designing their new products, only penetration testing will ensure that it has been implemented properly.

B. Product Costs

Axons latest product the Axon Body 3 list features such as live streaming, alerts, GPS, wireless activation. It has Bluetooth and WiFi Radio to connect to other devices that can act like a second screen or trigger events that start camera recording. These features however come at a pretty steep price. Aside from any data and networking storage costs, the Axon Body 3 starts at $699 per camera [8]. According the the Bureau of Justice statistics, the top 4 out of 5 reasons that an agency did not adopt body cameras was because of cost Fig. 1. Our solution will have to be cost effective as well as allowing for a rich feature set.

C. Device Connectivity

Police officers use on a wide variety of internet connected devices for background checks, vehicle registrations, dispatch orders, etc. Having strong, reliable, connection to maintain these services is important in our design.



Reasons for not having acquired body-worn cameras, by agency type, 2016

Reason	Total	Local police	Sheriff's office	Primary state police
Video storage/disposal costs	76.6%	76.7%	76.2%	71.0%
Hardware costs	74.4	73.3	78.7	64.5
Ongoing maintenance/ support costs	72.8	73.0	72.5	64.5
Public records request/video redaction costs	68.3	69.1	65.1	54.8
Privacy concerns	39.4	41.1	32.3	45.2
Training costs	38.8	38.6	39.6	29.0 !
Video transfer/storage issues	31.6	31.0	33.4	48.4
Liability concerns	25.0	26.1	21.0	19.4 !
Camera operation technical difficulties	18.3	18.1	19.2	19.4 !
No perceived need	13.3	13.9	10.8	35.5
Lack of support[a]	7.2	7.6	5.8	6.5 !
Other[b]	13.0	13.7	10.4	19.4 !
Number of agencies without body-worn cameras	8,069	6,420	1,613	36

Note: Details do not sum to 100% due to non-mutually exclusive categories. The categories of reasons given were provided as response options on the questionnaire, and agencies were asked to select all that apply. See appendix table 14 for standard errors.

! Interpret with caution. Too few cases to provide a reliable rate, or coefficient of variation is greater than 50%.

Fig. 1. Bureau of Justice statistics on why police agencies did not acquire BWCs [6].

III. Stakeholders

From the moment a police officer captures a video to the moment it reaches to the court as evidence, there are many stakeholders involved. The police officer is the one who initially takes the video. Once the shift is over, the police officer hands over the video to the police station. From there, an IT personnel inside the police department will log the video into the database. These are all the internal stakeholders who are directly involved in the Chain of Custody of the video. Similarly, when a video is requested in the court, the IT personnel sends it over to the lawyers, prosecutors and the judge. Therefore, each person will have a copy of the video. These are the external stakeholders who are involved in the chain of custody of the video.

IV. Requirements

1) Provide security services of non-repudiation, and verification from the point of evidence creation until evidence submission
2) Fix security problems addressed in industry wide flaws section
3) Provide better connectivity for devices in poor connection areas

V. Design

A. The Platform

Since the beginning of our development process, we wanted to choose a platform that had the most fully featured hardware/sensor suite and was easy to begin development on. Initially, we chose the raspberry pi for its many open source Linux libraries and modular sensor packages. While we were able to get a simple demo working with hashed video from the camera module, most other sensors required significant setup and were not power efficient for mobile use.

We then decided to use a mobile phone as development platform, because it is a pre-packaged development platform with all needed sensors and extensive development libraries. Another advantage is that firmware is already signed which solves one of the industry wide flaws in most BWCs. Where as the Axon Body 3 is $699, many fully featured android phones cost much less, which makes phones a cheaper platform as well. A police station can choose the best hardware that fits their budget constraints and performance needs.

Since all members of the team use iPhone's however, this became our development platform of choice. We created our app with the React Native as some of our members had experience developing with this JavaScript framework.

B. Identity Management

In our current model, the police station acts a CA and signs police officer certificates as valid users of BWCs. Each police officer has their own certificate installed on the device which is protected with a password only they know. In addition, the police station installs a certificate of their own for each device. Both of these certificates are stored and managed by the Apple keychain.

C. Signing Procedure

When metadata is ready to be sent to the police station, it requires two signatures 2. First it is signed by the officers certificate, and then by the police stations certificate. The first provides proof of Identity Verification and Validation of the officer, but does guarantee that the the metadata came from a specific device. The police stations device certificate ensures the metadata is coming from an authorized device as.

D. Non-Repudiation

To provide Non-Repudiation, requirements of *proof of origin* and *proof of receipt* must be met [9]. *Proof of origin* is already accomplished by the signing procedure above but *proof of receipt* is met when the CA sends back a signed hash of the metadata which is stored on the device.

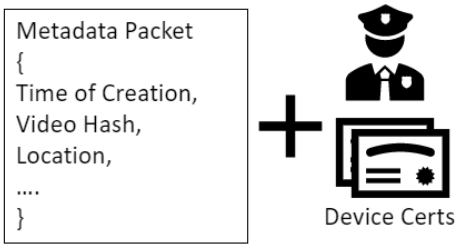


Fig. 2. Metadata

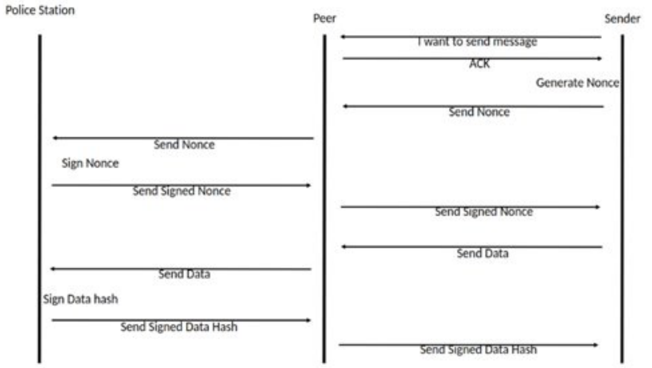


Fig. 3. Connection Protocol using P2P

E. Peer-to-Peer

To address requirement 3, we implemented a Peer-To-Peer(P2P) solution that can route packets through other devices when there is no connectivity to cell towers such as when inside a building.

When the app loses connectivity, it will automatically attempt to make Peer-to-Peer (P2P) connections with authorized devices. Apple's Multi Peer Connectivity framework is used to establish Wi-Fi Direct or Bluetooth connections with other devices and then a React Native Module wrapper is used to allow connection lifecycle hooks to be seen in the Javascript app. When not connected to the internet, the app will periodically scan for peer devices that broadcast if they are capable of forwarding the packet or not. Once it finds one, it will attempt to establish a connection.

To be considered a valid peer, each device must have a certificate that is signed by the police station signing certificate. Once the connection is established, the app will send its new hashes and metadata through the other device, which can forward it to a police station.

The connection protocol in Fig. 3 was created make sure that the device truly has connection to the police station and prevents it from performing replay attacks. While it stops replay attacks and provides non-repudiation, it will most likley be replaced with PSK-TLS in a future version. Due to limitations in the Multipeer Connectivity Framework, it was not possible to implement with out significant software development.

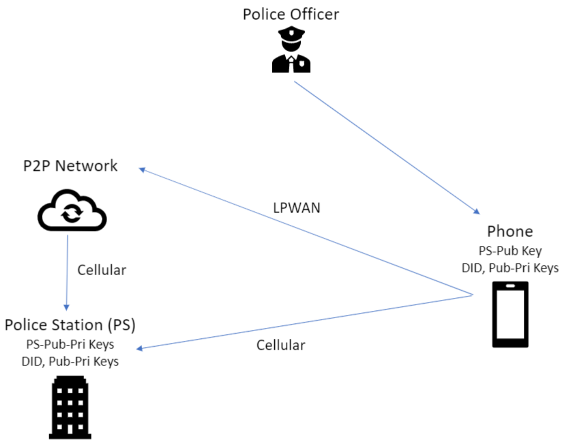


Fig. 4. Device connection Diagram

F. *Connection and Data Modes*

Aside from P2P, the app has two other connection modes: Cellular and Local. When the device has a cellular connection it will send data directly to the police station, otherwise it will enter the local state, where it stores data locally and begins searching for peers for P2P as shown in Fig. 4. Depending on data rates, the device can also send video clips in addition with metadata. Each clip is 5 seconds long and new metadata with a structure detailed in Fig. 5.

VI. CONOPS

The operation begins with the Police Officer who records the video. They are the temporary owner. It is then passed onto the authorized user allowed to view the evidence so in this case the Department. Lastly, it is passed onto the accessor which is the lawyer, judge, fellow officer who is in charge of checking the evidence and verify the chain of custody. Throughout this process, the evidence can only be handled by one party at a time. So once the initial police officer passes it, it is out of their hands.

VII. Implementation

The way we are implementing would be to get licenses needed for our code software that we used. With these developer licenses, we would be able to put the application on the Apple App store. From there our sponsor can coordinate with law enforcement agencies to test the product.

VIII. Verification and Validation

If our requirements are met, we can create a product that provides the security services that allow BWC evidence to be admissible in court, while being cost effective and simple to implement. It protects both officers and police stations from any foul play that might occur during operation.

While we achieved Requirement 1 for cellular connection, getting *proof of receipt* over P2P was not possible in the time frame. Requirement 2 was not possible given our development environment. Apple devices use the Bonjour protocol for P2P which does not allow the device broadcasting to hide their identity. An attacker may be able to detect devices and track police officers if the P2P protocol is being used. In addition, in our model, the Police Station is the manager of all evidence and hold the sole records that the evidence exists. This could leave it vulnerable to an insider threat unless, identity management is handled by a third party. A possible solution is discussed in the future works section. We completed Requirement 3 by switching to phones as a platform where firmware is already signed.

In order to conduct a more formal validation, our team would have to a pilot a test with Hexagon and a law enforcement agency and review feedback.

IX. Business Plans

Our business plans are to work with and use the open-source tools in order to optimize cost. This will help to develop our application as cost-effective. We would also like to expand on our application and get the application on the Apple App store and eventually to the Google Play store. We also would like to work with local Law Enforcement Police Departments.

X. Future Works

Due to time constraints, there were aspects of the project that were put off in favor of other core features. In this section we outline a more transparent system where neither officers nor police departments need to be trusted with maintaining evidence.

A. *Blockchain Identity System*

When videos are sent to a server for evidence storage, it is the responsibility of the department and server administrators to manage custody of the video. Both officers and judicial courts must trust these parties to carry out their job faithfully or else the whole system breaks.

In our current model, the department controls the single copy of the evidence. A malicious insider could delete evidence and remove any record that it was created.

To counteract this, an evidence blockchain can be used to issue certificates so no one party has access to all parts needed to make a properly signed video. In addition, it can maintain a record evidence that is distributed across many nodes with a consensus algorithm so no one server can make its own changes. These other nodes could be court systems, other police departments, or public record nodes. The metadata stored can be used to prove the videos existence, location, officer number, etc.

References

[1] C. Lum, M. Stoltz, C. S. Koper, and J. A. Scherer, "Research on body-worn cameras," *Criminology & Public Policy*, vol. 18, no. 1, pp. 93–118, 2019. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9133.12412

[2] C. R. Service, "Public trust and law enforcement—a discussion for policymakers," Congressional Research Service, Tech. Rep. R43904, 2018. [Online]. Available: https://crsreports.congress.gov/product/pdf/R/R43904

[3] P. Michael D. White, *Police Officer Body-Worn Cameras: Assessing the Evidence*. Washington, DC: Office of Community Oriented Policing Services, 2014.

[4] B. S. Shelley S. Hyland, Ph.D., "Body-worn cameras in law enforcement agencies," U.S. Department of Justice, Tech. Rep. NCJ 251775, 2016. [Online]. Available: http://www.bjs.gov/index.cfm?ty=pbdetail&iid=6426

[5] J. Mitchell. (2018, August) Ridealong adventures: Critical issues with police body cameras. DEF CON 26. [Online]. Available: https://www.youtube.com/watch?v=X34taF1R7sU

[6] I. T. Laboratory, "Digital signature standard (dss)," National Institute of Standards and Technology, Gaithersburg, MD 20899-8900, Federal Information Processing Standards Publication FIPS PUB 186-4, 2013. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.186-4

[7] N. B. L. J. M. D. Y.-Y. C. K. K. G. M. F. T. Paul A. Grassi, James L. Fenton, "Digital identity guidelines: Enrollment and identity proofing," National Institute of Standards and Technology, Tech. Rep. SP 800-63A, 2017. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-63a

[8] "2019 law enforcement agency pricing – axon systems." [Online]. Available: https://procurement.sc.gov/files/webfiles/Price%20List_Axon.pdf

[9] T. Coffey and P. Saidha, "Non-repudiation with mandatory proof of receipt," *SIGCOMM Comput. Commun. Rev.*, vol. 26, no. 1, p. 6–17, Jan. 1996. [Online]. Available: https://doi.org/10.1145/232335.232338