Privacy Enhancement via Adaptive Cryptographic Embedding

Balancing Liberty and Security in an Information Society

Walter Scheirer[1,2] – wjs3@vast.uccs.edu
Richard White[1] – rwhite2@uccs.edu
Terrance Boult[1,2] – tboult@vast.uccs.edu

Department of Computer Science
[1]University of Colorado at Colorado Springs
Engineering Building Room 199
1420 Austin Bluffs Parkway
Colorado Springs, CO 80933-7150

[2]Securics, Inc.
1867 Austin Bluffs Pkwy, Suite 200
Colorado Springs, CO 80918

Contact Phone Number: 719-387-0024

Privacy Enhancement via Adaptive Cryptographic Embedding
Balancing Liberty and Security in an Information Society

Walter Scheirer[1,2], Richard White[1] and Terrance Boult[1,2]
[1]University of Colorado at Colorado Springs and [2]Securics, Inc
Colorado Springs, CO. lastname@vast.uccs.edu

Table of Contents

Abstract

Significant research progress has been made in electronic surveillance, signals intelligence, and biometric identification that has increased the deployment and effectiveness of these technologies. For many, video domestic surveillance cameras, wiretapping and biometrics epitomize the (misperceived) "inherent" tradeoff between security and privacy, with staunch defenders of these technologies promoting them as indispensable tools for security and equally vocal groups that berate them as an ineffective siege. Congress, over the past thirty years, has enacted a slew of legislation to protect constitutional rights to privacy and speech, and other laws to provide for enhanced national security, yet little has been done to address, technologically, the

balance between liberty and security. While the balance of liberty and security is important, it is equally important to note that this is not a zero sum game or an inherent tradeoff. This paper presents a method that demonstrates the adaptation and application of cryptographic ideas to sculpt technological approaches that can move the "balance point" and provide simultaneous improvements to both security and privacy.

Privacy Enhancement via Adaptive Cryptographic Embedding (PEACE) is a method utilizing encryption techniques to improve privacy while allowing security applications to continue to use much of the data in context, and allowing full access (i.e. violation of privacy) only with possession of a decryption key. We introduce the application of PEACE in three areas: video surveillance, wiretapping, and biometrics. We present an in-depth case study for "warrantless" wiretapping, showing the details necessary for a new tool that protects both our country and the privacy of our citizens.

1. Introduction

All over the world, electronic surveillance is commonplace. People are forever under the watchful 'eye' of the camera - even as they go about their day-to-day activities. CCTV is widely used for surveillance in banks, parking lots, shopping malls, airports, and other public places. It is commonly accepted that placing video cameras in public places reduces the occurrence of criminal acts in those areas. Unfortunately, the misuse and abuse of surveillance video constituting an invasion of personal privacy is equally well documented.[1] Often times, cameras simply displace the security risk[2]. A USA Weekend survey[3] reported that 2,000 students were physically attacked each hour of the school day, and nearly half of those surveyed said they avoid school restrooms out of

fear. While cameras in school or airport bathrooms might improve security, the potential abuses prohibit their use.

Even the ability to video tape public events has its limits because of its potential to stymie political expression. The long standing Handschu class action suit in New York was recently reaffirmed by the US District Court, limiting the New York City Police Department's collection of surveillance video. While the initial ruling was slightly moderated after 9/11, the most recent decision[4] prohibits the NYPD's "recently implemented practice of videotaping public gatherings and preserving the videotapes," placing stricter guidelines on when and how video surveillance can be used.

Yet, video surveillance is only one facet of the surveillance dilemma. In the United States, the Bush administration's Terrorist Surveillance Program[5,6,7], recently brought the delicate balance between privacy and security back into the pubic eye. At stake is the Foreign Intelligence Surveillance Act (FISA), established in 1978 to curb warrantless tapping by the federal government. The act defines the boundary between warrant and warrantless surveillance, based upon the presence of American citizens or interests in the case. Shortfalls in the FISA program resulted in missed opportunities to thwart the 9/11 terrorist plot, prompting TSP, the USA Patriot Act, and the latest amendments to FISA. At dispute is the utility of a law enforcement tool, requiring due process and probable cause, for national security efforts attempting to prevent the next attack by intercepting the fleeting communications of a covert enemy. How do we reconcile national security requirements for casting a wide surveillance net against domestic civil justice requirements to only target specific individuals?

Beyond surveillance, we find other areas where the need for privacy and security

exists. Biometrics, used for authentication and verification, provide a powerful alternative to easily forgettable (and often times guessable) passwords and PIN numbers. The key properties of biometrics are also their Achilles' heel. While biometrics can initially improve security, as biometric databases become widespread, compromises will ultimately undermine the usefulness of biometrics for security. Compromised biometrics can be used either for generation of fake biometrics or to find someone that can be impersonated directly by an attacker. With many biometrics that have a "false accept" rate of .01% or even .001%, the security risks of both attacks at real. At least 40 million "financial records" were compromised or illegally sold in 2005[8]. As biometrics become widely used, databases with millions of permanent "non-revocable" biometric records will become a significant targets. With the current trend, it is a question of when, not if, a major biometric database will be compromised.

In this paper, we introduce an alternative to the current approaches for domestic surveillance that balances both security and privacy. Our technology-based approach is based on the notion of *adaptive cryptographic embedding*, which we describe in Section 2. While some previous work exists in other domains using the same concept to protect privacy, this is the first instance of it applied to surveillance for national security, which we describe in Section 3. In the case study presented in Section 4, a background to the portions of FISA and its amendments that are relevant to the discussion in this paper are presented, as well as our proposed solution, the *half-tap*. It is our intent in this paper to show that one need not compromise privacy for security – both can be established with the right technology and policy.

2. Privacy Enhancement via Adaptive Cryptographic Embedding (PEACE)

The general technique, that we term *PEACE*, is the technology that forms the basis of our proposals for protecting privacy while providing security for various applications. In recent times, security has become a dominant societal factor, with threats emerging from local, national, and international areas. In a basic sense, complete security is desirable in any domain requiring protection, but impossible to achieve for a variety of reasons. When evaluating security solutions with direct human contact, we must consider the impact a security measure will have on society – specifically, if it approaches a level of providing more harm than good. Risk assessments, especially in the short-term, tend to focus on their intended targets and actors, with little regard for other variables. If a low probability, but high impact risk exists, is it worth exposing a large population to privacy violations through the security design? Vulnerability through design encompasses several aspects including access use and controls, data accountability, insider actions, and outsider actions. In practice, we face tradeoffs (Figure 1) in designing these types of systems.

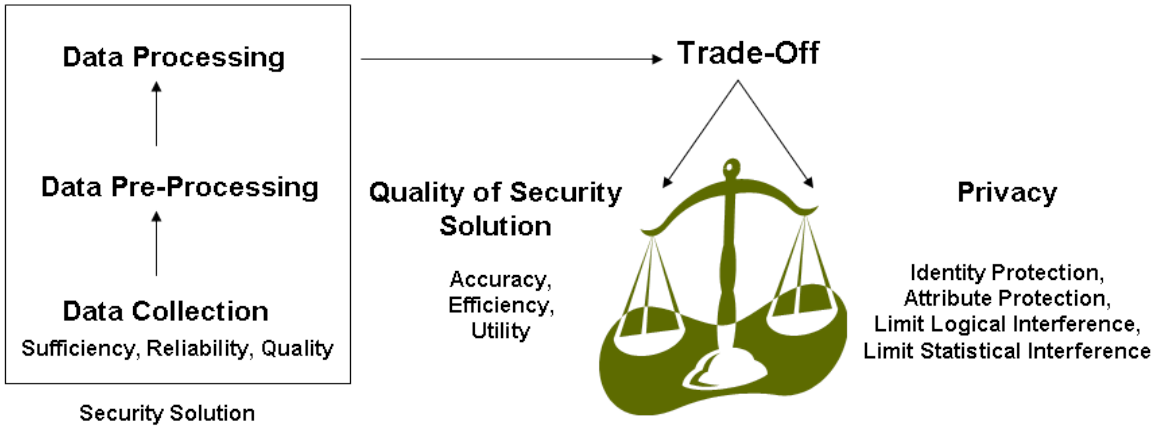

Figure 1. Making a Trade-Off in Security Design

With the above trade-off in mind, PEACE uses adaptive encryption to mask privacy information and keep constitutionally protected data private, while leaving all other information in the clear. In video applications, for example, PEACE can provide the same blurring, obscuring or distorting of confidential sources' faces and voices as we are used to seeing on TV. PEACE is different, however, in that the information is encrypted, not destroyed, thereby allowing full recovery of the protected data under lawful circumstances. The revolutionary advantage of this technical approach is that it allows unlimited intelligence collection, consistent with national security requirements, while protecting individual privacy, consistent with the Constitution and other laws (such as FISA, discussed later on in this paper).

The initial step in PEACE is to separate data into 3 classes:

- **Class 1: Minimum data needed to protect privacy**
- **Class 2: Data needed to achieve security objective**
- **Class 3: Data that is in both Class 1 and Class 2**

If Class 3 is empty and if Class 1 can be readily identified, then the data of Class 1 can be encrypted, while the rest is left untouched to support the security objective. If Class 3 is non-empty, we cannot simply encrypt the data of Class 1. Two alternatives exist for this scenario. First, we can attempt to minimize the extent of Class 3 through technology or policy (or both).

On the general idea of the separation of data into encrypted and unencrypted pieces, only one other group besides our own has explored the possibility. Yasukawa et al.[9] introduced a method of file system protection whereby files are divided into

segments, and these segments are selectively encrypted, in order to enforce some sort of protection. The primary domain targeted is copy protection for commercial software and media. This idea is akin to certain types of shareware, where a portion of a program is available free for public use, and the rest of the program remains missing or locked until a user pays for further access.

3. Application Areas for Homeland Security

3.1 Video Surveillance

As a first example of our work[10,11] with PEACE, we use face detection software to detect the faces in an image or video. The basic concept is a cryptographic extension of the obscuration idea; the potential private data is detected and the associated component of the media file is modified with the sensitive data encrypted in place. The goal is for the unencrypted data in the media to still be useful for general surveillance. Since the encrypted data appears as basically random numbers the associated part of the file simply appears (or sounds) like noise. This approach allows for surveillance in private areas that are generally off-limits for surveillance but prone to crime, and facilitates hard evidence for investigations. Public restrooms[12] are popular areas for petty crime, but they can also serve as a cover for more serious crimes if they are located in an airport or secure facility.

Figure 2. Privacy-enhanced surveillance. The person in the restroom is completely unidentifiable, but actions can still be observed. An authority with the appropriate access can decrypt the image.

In the example shown in Figure 2, regions around detected faces are encrypted and the encryption key and other details are saved as a structured comment. A decoding entity must have access to the private keys, which are stored in a secure, restricted manner. The decryption details are not publicly known, hence maintaining the privacy of the individuals in the video. But if the need arises, then all the details of the original face can be provided to authorized personnel. This aspect of recovering the original images from the transformed images is what makes our method unique from prior work. A digital signature of the image or face could be added to the comments ensuring traceability.

There are a few papers that discuss related work and propose methods to remove faces in surveillance video for privacy reasons, while leaving the rest of the scene intact. Newton et al.[13] discuss an algorithm called *k*-same to "de-identify" facial images and hence make the face(s) inappropriate for being used with face recognition software. In Senior et al.[14], the researchers have discussed their method of rendering face images unusable by face identification software. They suggest methods to obscure some facial features or alter the statistics of some facial features such that face recognition software cannot recognize the faces. Sony has a patent[15] in which they have proposed a method of detecting skin in images and replacing it with other colors, hence making it impossible to determine the race of the individual. Matsushita's patent[16] talks of a method to obscure a "privacy region" of an image as seen on camera. None of these schemes support original data recovery under the appropriate circumstances. Without the ability to recover the original data, the ability to use them to identify and prosecute suspects is removed, and so is the deterrent value of the surveillance.

3.2 Biometrics

In the biometrics realm, the idea of privacy preserving biometrics, or revocable biotokens has gained a great deal of traction recently. The fundamental dilemma is that unlike a password or PIN, biometric data cannot be regenerated once compromised. Moreover, biometric data automatically links the owner of the data to its use – a property that is either desirable or undesirable, depending on the application. The threat of unprotected biometrics is clear. A low security area, such as a gym may collect biometric data and store it in insecure manner. A member of the gym may have access to a secure facility, which requires a biometric sample for access. If the gym's database of biometric data is compromised, an attacker may be able to access the secure facility. Revocable biotokens solve this problem by being unique per application, meaning the gym's data could not be used to access the secure facility.

Our work[17,18] in this area shows the successful application of adaptive cryptographic embedding to create *revocable biotokens* from face and fingerprint features. Biometric features are inherently unstable, but possess an overall characteristic of stability, with minor variability (the structure of a fingerprint will not change significantly over a lifetime, but minor changes, such as scars or wear, will inevitably occur). For our PEACE approach to biometrics, we separate the data into a stable portion and an unstable portion, and encrypt the stable portion, leaving the unstable portion in the clear. This transformation protects the privacy of the owner of the biometric features, while still supporting accurate matching of tokens in the encoded space. The resulting tokens can be revoked and re-issued in the same manner as digital certificates, allowing for a PKI-like infrastructure for secure transactions[19].

In the biometric realm, a few approaches for cancelable or revocable biotokens have been discussed in the literature, with a review and classification of the leading prior work presented in the work of Ratha et al.[20]. They divide the field into four categories: Biometric salting, Fuzzy schemes, Biometric Key generation and non-invertible forms. Our approach, as applied to biometrics, does not fit within any of these categories, and does not suffer from the proposed attacks[21] to such schemes.

3.3 Communication

There is nothing preventing a communications channel from being separated into discrete parts, each representing a party participating in the "conversation." In a telephone call, these parts are simply voice channels. In an Internet data connection, a party may be the client or server side of the connection. During the proposed privacy-preserving a wiretap, once channels have been separated, and their origins identified (to some degree of confidence), the law must be considered for the further treatment of each channel. If the channel is that of a foreign party, American laws do not apply, allowing for immediate analysis of the content. If the channel is of domestic origin, it is immediately encrypted, with keys held in the possession of a panel of judges. If an investigator desires access to this encrypted channel, an appeal must be made to the panel of judges - perhaps bolstered by evidence obtained from the unencrypted, foreign channel, or data obtained after the call. A series of judges, not just a single judge, must provide their unique keys for decryption, making it very difficult for a rogue investigator to circumvent the process. For legitimate requests, a warrant will be granted, providing access to the decrypted channel for the investigator.

Implemented within a robust policy framework, PEACE provides a technological

solution to the current security dilemma ensuring more stringent adherence to privacy laws than previous legislation alone. Privacy information remains always protected by physical encryption against those who might try to access it outside the law. Some civil libertarians are already in favor of security[22], if rigorous monitoring takes place to ensure that any surveillance program conforms to the law, which maintains absolute authority over evidence collection and use.

PEACE allows unlimited intelligence collection within the constraints of FISA, while upholding the constitutional protection of individual privacy and speech. It must be acknowledged that FISA, as it stands today, is dated. Communications networks were not nearly as large or widely deployed in the 1970s, as they are today. The consequence of the telecommunications boom on the 21st century is that analysts tied to the current FISA system are at a disadvantage when attempting to collect timely intelligence. By allowing warrantless taps, with the exposure of only the foreign portion of the communication, analysts are immediately given an important piece of information, and added material to use in obtaining the FISA warrants. In addition, the American side of the data was captured, in encrypted form, so while there may be a short loss of time, there need not be any loss of data. To date, there is no similar work to our PEACE solution for the warrantless wiretapping dilemma. In the next section, we present a thorough case study on this matter.

4. Case Study: Half-taps

4.1 The constraints of FISA and its Amendments

FISA provides a framework for the use of electronic surveillance, physical

searches, pen registers and trap and trace devices to acquire foreign intelligence information.[23] Pen registers, and trap and trace devices are a kind of secret "caller id", which identify the source and destination of calls made to and from a particular telephone.[24] All electronic surveillance for counterintelligence purposes within the United States is subject to the requirements of the FISA. This does not mean, however, that prior judicial authorization is always required. The Attorney General may acquire foreign intelligence information for periods up to a year without a judicial order if the Attorney General certifies in writing under oath that:

(A) the electronic surveillance is solely directed at . . . communications used exclusively between or among foreign powers. . . [or] technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power . . .;

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures . . . meet [the statutory definition] of minimization procedures . . . .

The FISA establishes a much more stringent standard in circumstances involving the electronic surveillance of "United States persons." In such circumstances, the Executive may conduct electronic surveillance only pursuant to the FISA's procedures for judicial review and approval.[25]

Each application approved by the Attorney General for the electronic surveillance of United States persons within the United States must have judicial approval. The Chief Justice of the United States Supreme Court has designated seven federal district court

judges to be the Foreign Intelligence Surveillance Court (FISC) and to review the electronic surveillance search applications. A FISC judge will approve the electronic surveillance application and issue an ex parte order upon a finding that: (1) "the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;" (2) an authorized federal official made the application and the application was "approved by the Attorney General;" (3) there is probable cause to believe that the target is "a foreign power or an agent of a foreign power" and that each place subjected to surveillance "is being used, or is about to be used, by a foreign power or an agent of a foreign power;" (4) "the proposed minimization procedures meet the [statutory] definition of minimization procedures . . . ;" and (5) all required statements are contained in the application and, "if the target is a United States person, the [statutory] certification or certifications are not clearly erroneous . . . ."[25]

This statutory regime worked well during the Cold War for conducting surveillance on spies who were either foreign nationals employed by foreign government working under diplomatic cover at foreign embassies in the United States, or United States persons in this country who had been recruited to spy by foreign intelligence agencies. Both were clearly "agents of a foreign power," and gathering foreign intelligence on the activities of these targets was generally the "primary purpose," if not the only purpose, of the surveillance.[26] The statutory regime has not worked as well with respect to terrorists, who did not work for a foreign government, who often financed their operations with criminal activities, such as drug dealing, and who began to target American interests. It has become more difficult to determine if such terrorists are "agents of a foreign power" and it was difficult for the government to keep the

appropriate types of investigators, intelligence or criminal, involved in the operation.[26]

The new amendments to FISA[27] address major problems associated with the original Terrorist Surveillance Program. Telecommunications providers who provide assistance to the federal government for domestic wiretaps are now granted immunity from lawsuits brought forth in response to such assistance. More importantly, a seven day window (expanded from three days) is now granted to investigators to tap the communications of foreign nationals, without a warrant, in cases where a direct threat to national security is believed to exist. The new amendments also solidify the FISA as the exclusive means of conducting domestic wiretapping for intelligence purposes. Unfortunately, these changes do not grant investigators and analysts the flexibility they need to protect the United States from future attacks, nor do they protect innocent American citizens from being tied to suspicious persons, and having unrelated private information divulged. PEACE can make the necessary difference.

4.2 Operational Details of the Half-Tap

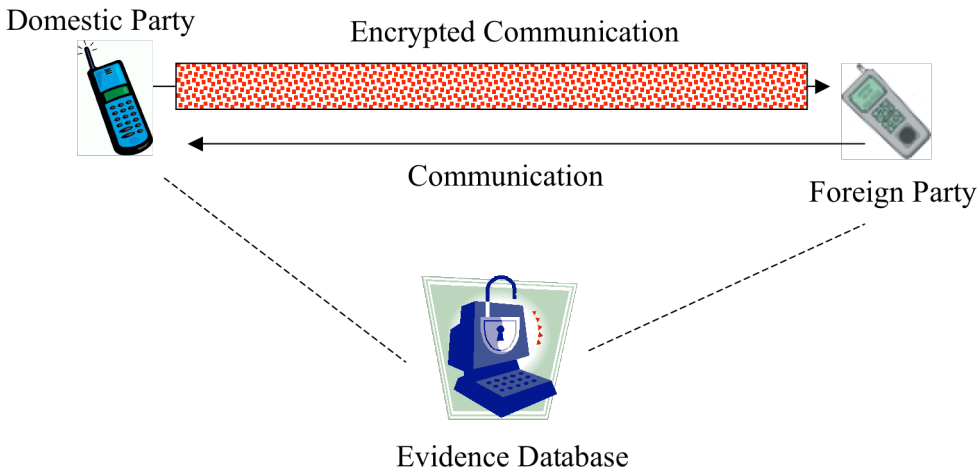

Figure 3. Protecting domestic communication in a warrantless but privacy preserving half-tap

PEACE can make a difference in support of warrantless, privacy preserving

wiretaps. Figure 3 depicts a two-way communication link between a domestic and foreign party. Voice and data traffic on telecommunications networks adapts nicely to our data separation technique, since there is a distinct division between the parties involved in the connection. As the communication proceeds, a surveillance monitor encrypts the domestic party's channel, while leaving the foreign party's channel in the clear. This allows for immediate intelligence analysis on half of the communication, which, if deemed critical, can lead to a request for a warrant to unlock the remaining piece. This scheme is in full accordance with the rules of the FISA, which protects American citizens, but grants no such protection to "foreign powers"[28]. The details of how this should be implemented at the telecommunications provider are depicted in Figure 4.

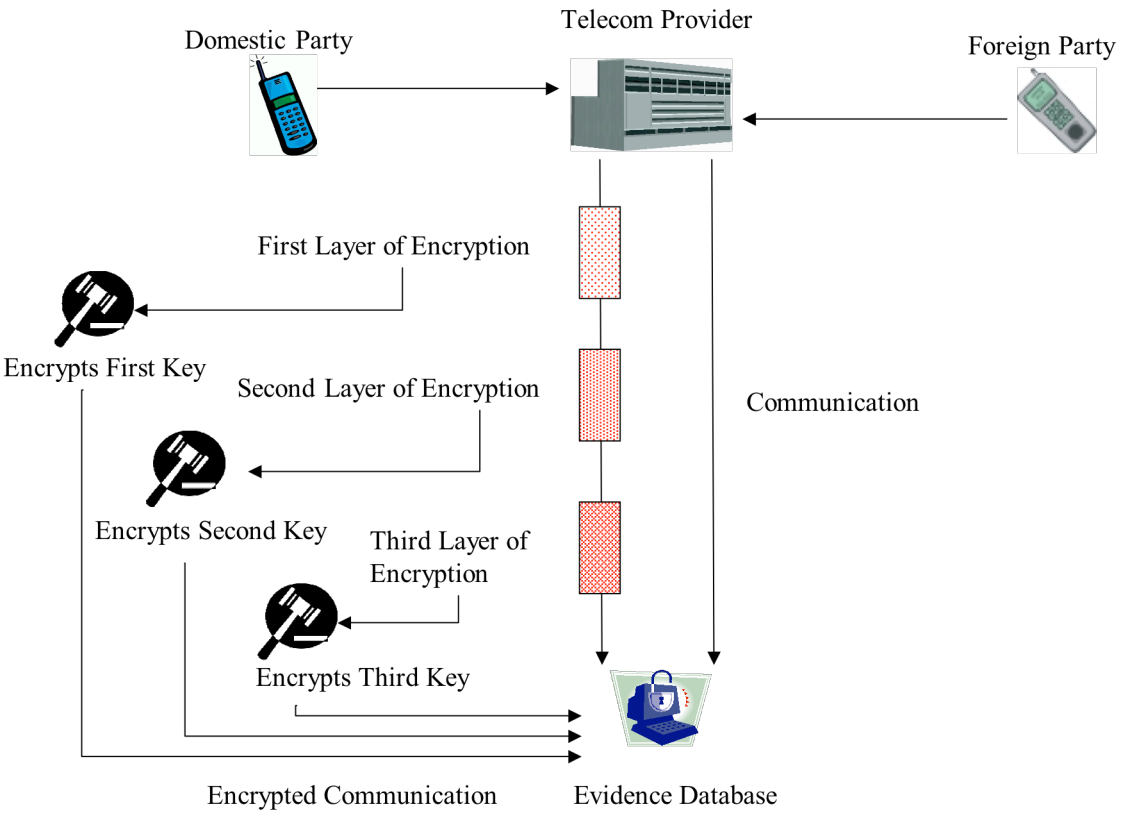

Figure 4. Evidence collection at the telecommunications provider

Acts such as CALEA[29] already provide an infrastructure for telecom surveillance. We describe an enhancement to such infrastructure in Figure 4. The foreign channel is passed in the clear to a central evidence database, while the domestic channel is subject to multiple rounds of encryption. In this example, three encryption keys are generated and used to encrypt the domestic channel three times. Each of these session keys is then encrypted by a particular judge, and stored in the database with the final encrypted form of the domestic channel. Thus, if the domestic channel is to be decrypted, three judges must consent to grant a warrant. This is shown in Figure 5.

Figure 5 depicts two attempts at evidence recovery: with and without a warrant. On the left, an intelligence official without a warrant attempts to access the domestic channel. This investigator is completely unsuccessful in this pursuit, because no decryption keys are available to recover the original data. On the right, an intelligence official with a warrant is able to obtain all three session keys from the judges who, after granting the warrant, have decrypted them using their own keys. With all three keys used to encrypt the domestic channel in hand, the official is able to decrypt the data, and recover the original domestic communication. An alternate approach to evidence recovery, with the judges performing the decryption, is also possible[30].

The process for obtaining a warrant aids the intelligence analyst considerably. A much wider "surveillance net" can be cast, compared with the current FISA arrangement. With half the communication available, the probability of finding compelling evidence if the call is truly suspicious is high. Figure 6 shows this process, with a keyword search applied to the foreign party's communication channel. If suspicious terms are found, an appeal can be made to the judges, who will decide if a warrant should be granted to

decrypt the domestic half of the call. This process enhances security while preserving the privacy guaranteed by the law.

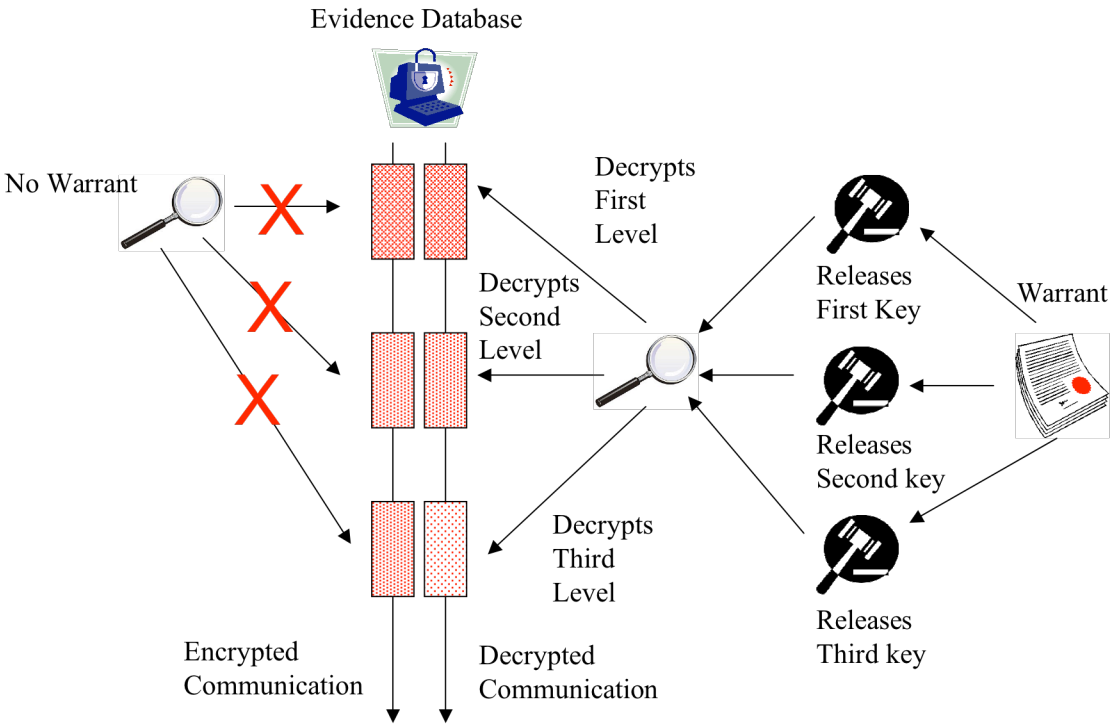

Figure 5. Recovery of evidence with judges providing keys

The process can be further extended to have audio filters applied prior to the encryption (particular keyword detection or stress level analysis). Different types of summaries of that analysis, from statistical counts to actual keywords, might also be encrypted, but with a lower bar to get to access that data (plausible suspicion rather than probable cause). Such "decrypted summary data" might then be combined with the foreign communication data to enhance the request for a full decryption warrant.

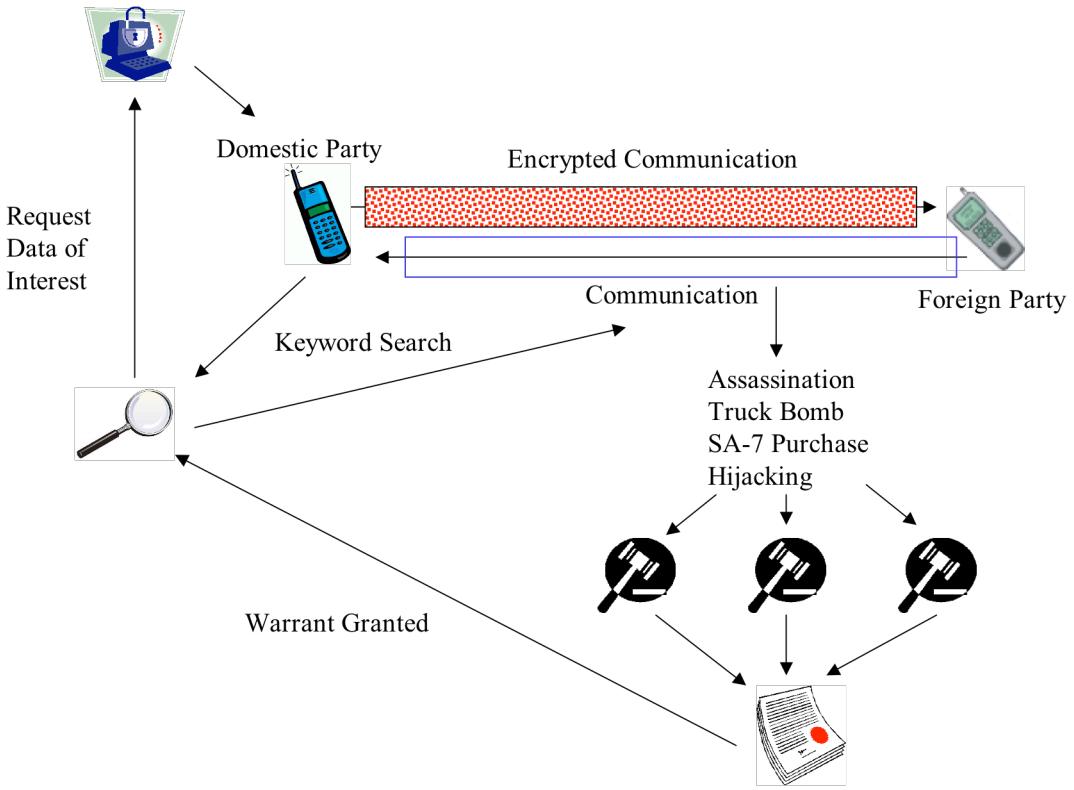

Figure 6. Obtaining a warrant

Clearly, technology is not infallible, and the potential exists in this scheme for circumvention at multiple levels (at the direct tap of the communication line, corrupt telecommunications employees, and corrupt judges, to name just a few). In order to account for potential compromise, the entire evidence collection process will be detailed in an audit log. Each step must have a corresponding discrete log entry. Thus, when one queries the evidence database, it can be known who has accessed and modified the data, as well as who is responsible for key control. More importantly, this log must be presented when action is taken against suspects based on the evidence gathered, whether it is an arrest or trial proceeding. We acknowledge that evidence can be collected outside this framework, which is why the existence of the audit log is crucial. If a legitimate log

cannot be presented, the case against the suspect must be dropped, and prosecution should be taken up against those responsible for circumventing the protections presented here.

5. Conclusion

The balance between liberty and security can be obtained with today's technology. In this paper, we introduced the notion of *Privacy Enhancement via Cryptographic Embedding*. The idea of PEACE is intuitively simple – we separate data into three classes, based on what needs to be protected, what is needed for security, and what satisfies both conditions. Data that needs to be protected is encrypted, while everything else may be left in the clear. Through our three main application areas, we noted the power this approach has to solving the timely homeland security problems of video surveillance, wiretapping, and biometrics.

In our case study, we have taken a survey of the problems associated with the current domestic wiretapping provisions, introduced the notion of privacy enhancement via adaptive cryptographic embedding, proposed the alternative of privacy persevering half-taps, and introduced the full operational details for privacy preserving half-taps. It is our hope that this proposal will be taken seriously by policy makers and civil libertarians alike. The answer to the question of whether it is possible to gather useful intelligence without compromising the privacy entitled to American citizens is a resounding - yes!

Bibliography

[1] Andrew Senior, Sharath Pankanti, Arun Hampapur, Lisa Brown, Ying Li Tian, Ahmet Ekin (August 2003). "Blinkering Surveillance: Enabling Video Privacy Through Computer Vision," IBM Research Report, August 28, 2003

[2] Jennifer King, Deirdre Mulligan, Steven Raphael, Travis Richardson, Jasjeet Sekhon, "Preliminary Findings of the Statistical Evaluation of the Crime-Deterrent Effects of the San Francisco Crime Camera Program," University of California at Berkeley, March 17th, 2008

[3] Leslie Ansley, "Safety in Schools: It Just Keeps Getting Worse," USA Weekend Magazine, August 13-15, 1993, pp. 4-6.

[4] Judge Haight, of the United States District Court in Manhattan, 71 Civ. 2203 (CSH), Memorandum Opinion and Order, February 15, 2007

[5] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Caller Without Courts," The New York Times, December 16th, 2005.

[6] Eric Lichtblau, "Despite a Year of Ire and Angst, Little Has Changed on Wiretaps," The New York Times, November 25, 2006

[7] United States District Court, Eastern District of Michigan, Southern Division. 2006. Reference re American Civil Liberties Union et al. v. National Security Agency.

[8] Jonathan Krim and Michael Barbaro, "40 Million Credit Card Numbers Hacked," Washington Post, Saturday, June 18th, 2005.

[9] Hiroshi Yasukawa and Takashi Kurosawa (November 1995).

"Method and apparatus for protecting widely distributed digital information," US Patent 5,999,622, Microsoft Corporation, November 22, 1995.

[10] T. E. Boult, "PICO: Privacy through Invertible Cryptographic Obscuration," IEEE/NSF Workshop on Computer Vision for Interactive and Intelligent Environments, Nov 11, 2005.9

[11] A. Chattopadhyay and T. E. Boult, "PrivacyCam: A Privacy Preserving Camera using uClinux on the Blackfin DSP," Third IEEE Workshop on Embedded Vision Systems, June 2007

[12] Leslie Ansley, "Safety in Schools: It Just Keeps Getting Worse," USA Weekend Magazine, August 13-15, 1993, pp. 4-6.

[13] Elaine Newton, Latanya Sweeney, Bradley Malin (March 2003). "Preserving Privacy by De-identifying Facial Images," Technical Report, CMU-CS-03-119, Pittsburgh, March 2003. Retrieved October 25, 2004, from http://privacy.cs.cmu.edu/dataprivacy/projects/video/CMU-CS-03-119-600dpi.pdf

[14] Andrew Senior, Sharath Pankanti, Arun Hampapur, Lisa Brown, Ying-Li Tian, Ahmet Ekin (August 2003). "Blinkering Surveillance: Enabling Video Privacy through Computer Vision", IBM Research Report, August 28, 2003

[15] A. M. Berger (May 2000). "Privacy mode for acquisition cameras and camcorders", US Patent 6,067,399, Sony Corporation, May 23, 2000

[16] Jyoji Wada, Koji Kaiyama, Ken Ikoma, Haruo Kogane (April 2001). "Monitor camera system and method of displaying picture from monitor camera thereof," European Patent, EP 1 081 955 A2, Matsushita Electric Industrial Co. Ltd., April 2001

[17] T. E. Boult, "Robust distance measures for face recognition supporting revocable biometric tokens." IEEE Conf. on Face and Gesture, 2006.

[18] T.E. Boult, W. J. Scheirer, and R. Woodworth, "Secure Revocable Fingerprint Biotokens," to appear in Proc. of CVPR, Minneapolis, June 2007.

[19] W. J. Scheirer and T. E. Boult, "Bio-cryptographic Protocols with Bi-partite Biotopes," Technical Report, VAST lab, University of Colorado at Colorado Springs, 2008, from: http://www.vast.uccs.edu/DOCS/wiretaps-article.pdf

[20] N.K. Ratha,, S. Chikkerur,, J.H. Connell, and R.M. Bolle. "Generating cancelable fingerprint templates," IEEE PAMI 29(4), 561-572, 2007

[21] W. J. Scheirer and T.E. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," in the Proceedings of the 2007 IEEE Biometrics Symposium, Baltimore, MD

[22] Marc Rotenberg and Kim Taipale, "Balancing Privacy and Security," The Wall Street Journal Online, May 16th, 2006.

[23] Bazan, Elizabeth B., "CRS Report for Congress: Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions," Congressional Research Service, United States Library of Congress, September 22, 2004, pp. CRS-8 – CRS-9.

[24] Doyle, Charles, "CRS Report for Congress: The USA Patriot Act: A Legal Analysis," Congressional Research Service, United States Library of Congress, April 15, 2002, pp. CRS-4.

[25] Chiarella & Newton, "So Judge, How Do I Get That FISA Warrant? The Policy and Procedure for Conducting Electronic Surveillance," *The Army Lawyer*, October 1997, pp.

[26] Hatch, Orrin, "U.S.A. Patriot Act," Congressional Record, September 24, 2002.

[27] H.R.6304, "To amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes," introduced June 19th, 2008

[28] 50 U.S.C. Chapter 36 Foreign Intelligence Surveillance.

[29] Communications Assistance for Law Enforcement Act of 1994. Pub. L. No. 103-414, 108 Stat. 4279.

[30] W. J. Scheirer and T. E. Boult, "Privacy Preserving Half-Taps," Technical Report, VAST lab, University of Colorado at Colorado Springs, 2008, from: http://www.vast.uccs.edu/DOCS/wiretaps-article.pdf

Author Biographies

Walter Scheirer

Walter Scheirer received his M.S. (computer science) and B.A. (computer science and international relations) degrees from Lehigh University, focused in security. He is a 3rd year Ph.D. candidate at UCCS working in biometrics, and the lead Biometric Engineer at Securics, Inc. He has published and lectured widely on a variety of security related topics, including face detection for surveillance, privacy enhancing technologies, secure cryptographic channels, network intrusion detection, forensics, and Unix system security.

Richard White

Rick White is Assistant Director for Curriculum Development at the UCCS Center for Homeland Security. Rick taught military strategic studies at the Air Force Academy before retiring in 2004. In 2006, he produced a textbook on the Department of Homeland Security, followed by a textbook on Homeland Defense. Since 2005 he has developed and taught national and international programs in HS, and is presently working on a Ph.D. in Security at UCCS.

Terrance Boult

Dr. Boult is the El Pomar Endowed Chair of Innovation and Security and Professor of Computer Science at UCCS, as well as the co-founder and CEO/CTO of Securics, Inc. Dr. Boult has published over 150 papers and holds 7 patents, with 9 patents pending. His on going research projects include advanced biometrics, advanced visual security

systems, network security, and embedded vision/surveillance platforms. Prior to joining UCCS, Dr. Boult held appointments at Columbia and Lehigh University.