Good example of research paper on program or issue

Law, Criminal Justice

PATRIOT Sunsets Extension Act of 2011 allows for roving wiretaps similar to the ECPA, effectively enabling spies to intercept a suspect's electronic and wire communications associated to suspect conduct under the PATRIOT Act 2000, regardless of their location. This helps track suspects who move from phone booth, handset or computer to computer multiple times in order to foil tacking efforts. Roving wiretapping necessitates interception of email communications (without naming the communications carrier and other third parties involved in the tap). Section 209 allows stored voice mail to be treated as data as defined under section 2703 as against intercepts defined by the procedures of wiretapping. This harmonizes the manner through which e-mail and voice mail messages may be accessed without a Title III authorization.

Further, the PATRIOT Sunsets Extension Act of 2011 explicitly clarifies that foreign intelligence surveillance is separate from the ECPA-protected procedure besides making it easier/possible to pen register or trap and trace surveillance under the Foreign Intelligence Surveillance Act (FISA). It also allows government investigators a potentially broad access to the types of items that may be subject to FISA subpoena, including servers. The Act specifically provides that pen register /trap tracing is applicable to the internet traffic, besides allowing for nationwide service of process and requires due reporting on the use of carnivore-type technologies. Carnivore-style technologies refer to those involving the installation and use of own pen register/trap and trace device(s) on packet-switched networks. By the tangible records provision under this Act, telecoms, libraries, banks, securities brokers, credit-rating agencies, dealers regulated by the Securities

and Exchange Act (1934) are mandated to turn over customer information to the government on request even if it overrides the privacy guarantees/requirements (i. e. without obtaining the customer's consent). The " lone wolf" provision also expands surveillance of an entirely new category of individuals as defined under FISA's " agents of foreign powers". This includes individuals engaging in international terrorism or related preparatory activities, effectively allowing the government to target foreign citizens without existing ties to a known terrorist group or other entity. This allows for legal surveillance on any individual in the world, even without any evidence of their involvement in terror activities or having known ties to a terrorist organization or other alien power. The key challenge in this case to provide a technological basis for the government (law enforcement agencies) to implement the PATRIOT Sunsets Extension Act of 2011 in an effective and efficient manner, within the legal bounds defined by the act as well as the wider PATRIOT ACT. Any such technical platform needs to bear into consideration the available and future surveillance technologies, while at once ensuring that it is reasonably possible to ensure that the privacy of the privacy of both the targeted suspects and other members of the public is protected to the best extent practicable.

Program Requirements

The program needs to capture, store and process large amounts on communications. These communications (voice, video, or text communications) need to be captured in real-time or near real-time if the data collected must be useful in identifying and preventing terrorist and other attacks against the United States. Firstly, part of the data capture

mandated under the tangible records provision is easy, not least because private entities may volunteer data and information in good faith, but also because they may be requested to turn over any data that investigators may be interested. Effectively, gathering data in this manner is easy but given the huge amounts of data that this could potentially provide, processing and analysis of the same presents a challenge. However, this challenge needs to be addressed in the broader context of the surveillance program.

Capturing data by wiretapping is relatively more difficult, but even more important in target identification. Law enforcement is heavily reliant on non-content communications records that show locations, contacts and movement. Investigators at a local and national level need to intercept, capture, store, process and analyse data. The data may be drawn both from ordinary conversations e. g. by use of eavesdropping bugs in rooms. The vast majority of the data is obtained from telephone and electronic communications (including e-mail, video, stored data, VoIP, video conferences, online social networking data, filter transfer, and notifications about targeted activities). There are tried-and-tested wiretapping technologies including planting microphones and web cameras in the suspects' homes have a role to play, but there are technologies that have already been developed to mitigate against this risk, which will in turn result in a failure to collect valuable intelligence. In the United States, the Communications Assistance for law Enforcement Act (CALEA) requires communication service providers to design their networks to ensure national security and law enforcement officers are able to perform legal electronic surveillance at the premises of the service providers (who include traditional

telecommunications providers, facilities based broadband internet service providers and interconnected VoIP service providers). Effectively, the proposed program needs fully to utilize this opportunity.

Further, the “ lone wolf” provision extends the surveillance efforts to individual citizens across the world, who require the deployment of endpoint systems, which will extend wiretapping to peer-to-peer services such as VoIP services. This is important especially since the increasing use of mobile and internet services makes it difficult to pin down a suspect to a single provider (Adida et al., 2013). Other requirements by this program include:

- The ability to legally override technical cyber security barriers installed by possible suspects and other entities that may prevent access to the target electronic communications. This necessitates the introduction of new ethical protocols to facilitate accountable wiretapping within the context of the Act.

- An auditing infrastructure to avoid abuse of data or information gathered through the surveillance operation, including through the implementation of auditing, reporting and compliance verification protocols to protect the confidentiality of gathered records as well as ensuring the integrity of any data gathered in this manner.

- Full utilization of software and hardware vulnerabilities to gather data and information from suspects (Landau, 2005)

- Prevent the introduction of new cyber security vulnerabilities created as a result of the requirement to facilitate surveillance from being exploited for fraud or other abusive purposes

Technological Requirements

Data Mining

Data obtained under the tangible records provision may be analysed using a range of data mining and analysis tools available on the market, including those that are open-sourced. Investigators may request for copies of emails, chats and other communications from banks, libraries and other businesses such as Facebook, Google, Microsoft and the Royal Bank of Scotland, which is subsequently analysed (Landau, 2005). Proprietary open-sourced systems include Orange, GATE Natural Language Processing, Massive Online Analysis and SPMF among many others. These systems employ a range of techniques including content filtering, machine learning and natural language processing to track trends and persons of interest automatically.

Wiretapping

Since telecoms are required to include wiretapping capabilities within the switching mechanisms under CALEA II, collectively known as ANSI Standard J-STD-025 or the J-Standard, which standardise the manner in which wiretap information may be communicated to law enforcement agencies (Adida, et al, 2013). The architecture is shown in the figure 1 below. Every subscribed service links to the service provider’s switchboard. The switch communicates the subscribers’ communications across the network, and in the event that the subscriber is under surveillance, the CALEA II-compliant switching system would convey a copy of the communication to the Delivery Facility, from where the data is transferred using the J-Standard protocol to the law enforcement agencies at a local or national level. This includes ISDN, D-

Channel Services, Narrow Advanced Mobile Phone System, Packet Data TDMA, TCP/IP services and paging services among other protocols. The J-Standard protocol encrypts the information according to a system accessible by law enforcement agencies. Call metadata is sent to investigators separately.

Figure 1: Wiretapping architecture under CALEA

Exploitation of Vulnerabilities

However, rapid technological changes and mobile IP-based communications have seen increasing encryption and reliance on peer-peer communication methods, which prevent wiretapping, not least because some software/hardware is open sourced or developed outside the United States. Targets that move from the service provider (WI-FI network) to another would be difficult to trace, without peer-to-peer surveillance (Landau, 2005). Fortunately, communications' devices used hardware and software platforms that have inherent weaknesses, which may be legally exploited by law enforcement agencies. Law enforcement agencies can develop exploitation tools for specific vulnerabilities, which can facilitate the installation of a wiretap code on the host machines, which subsequently gather and relay information to law enforcement agencies. Federal law enforcement agencies are best placed to accomplish this. These will be targeted at all the popular communication applications.

Implementation Support System

Data mining and vulnerability exploitation technologies are best implemented at a county, state and federal, because of the considerable

resource requirements and the fact that any surveillance techniques developed at this level may be accessed by other law enforcement agencies. The support system should include:

- Creation of federal, state and county law enforcement laboratories to help law enforcement agencies remain ahead of changing technologies. The labs should be capable of developing and deploying (law-enforcement-grade) tools to identify and exploit hardware/software vulnerabilities (Bellovin, Blaze, Clark, & Landau, 2013). Given the rapid technological changes and rapid changes in the techniques deployed by potential terrorists, this is critical.
- Establishment of a legal team to advise law-enforcement agencies on compliance, risk identification and mitigation
- Since individuals within the law enforcement system may require specific legal and technical training
- Maintenance of equipment and systems used for surveillance purposes, which requires in-house or contracted software and hardware engineers, network engineers.

Prospective Issues

Security is a critical concern for communication systems, but this can be easily undermined through the exploitation of vulnerabilities that are already known to law enforcement agencies. Ethical problems arise regarding whether law enforcement agencies should work towards the patching up vulnerabilities or exploit them. Further, lawful interception technologies and procedures include features that are specifically designed to breach the

confidentiality of communications. In addition, the potential for abuse of government surveillance practices remains high as perhaps best emphasized by the Edward Snowden revelations of practices by the National Security Agency. The requirement of warranties, conditioned on probable causes before wiretaps and other forms of surveillance may be deployed must be abided by at all times.

Internet communication has gained popularity over the recent decades, which presents a unique surveillance challenge. Other than the proliferation of internet-based communication applications, payload communications for surveillance have moved from central control points to the end-points (peer-to-peer systems). The versatility of endpoint systems is a challenge that would remain difficult to overcome within the current bounds of the PATRIOT Sunsets Extension Act of 2011. It may be necessary for the future to require systems that are pre-designed for surveillance purposes.

References

Adida, B., & et-al. (2013). CALEA II: Risks of Wiretap Modifications to Endpoints. Center for Democracy & Technology.

Bellovin, S. M., Blaze, M., Clark, S., & Landau, S. (2013). Going Bright: Wiretapping without Weakening Communications Infrastructure. IEEE Security & Privacy, vol. 11, no. 1, 62-72.

This article captures the difficulty associated with internet surveillance because rapid technological changes and mobile IP-based communication methods, which have rendered wiretapping increasingly harder. The authors argue that this has resulted in the need for the redesign of wiretapping

requirements applicable to digital voice networks to IP networks infrastructure. However, Bellovin, Blaze, Clark, & Landau (2013) argues that this approach to surveillance creates massive security problems, which is why investigators should always rely on vulnerability exploitation. Bellovin is a researcher and academics at Cumbria University, while Blaze and Clark teach at the University of Pensylavannia. Landau is an experienced cybersecurity, public policy and privacy expert.

Das, S. K., Kant, K., & Zhang, N. (2012). Handbook on Securing Cyber-Physical Critical Infrastructure. London: Elsevier.

This book gives a perfect overview of the security threats presented by the internet revolution, the need for surveillance, technical approaches to surveillance and the associated difficulties. It gives theoretical foundations and practical solutions to ensure the security of the physical and cyber infrastructure among others. Sajal K. Das is a director at the Center for Research in Wireless Mobility and Networking and head of department at the University of Missouri, while Kant and Zhang are equally highly experienced academics and widely published authors in the field.

Landau, S. (2005). CALEA and Network Security: Security, Wiretapping, and the Internet. New York: EEE Security and Privacy.

Landau, S. (2005). Security, Liberty and Electronic Communications. Seattle: Sun Microsystems.