Proceedings of the 2006 IEEE
Workshop on Information Assurance
United States Military Academy, West Point, NY

Battery-Sensing Intrusion Protection System

Timothy K. Buennemeyer, *Student Member, IEEE*, Grant A. Jacoby, *Senior Member, IEEE*, Wayne G. Chiang, Randolph C. Marchany, *Member, IEEE*, and Joseph G. Tront, *Senior Member, IEEE*

***Abstract*—This paper proposes an innovative Battery-Sensing Intrusion Protection System (B-SIPS) for mobile computers, which alerts on power changes detected on small wireless devices. These hosts are employed as sensors in a wireless network and form the basis of the "Canary-Net" intrusion detection system (IDS). This detection capability is scalable and complementary with existing commercial and open system network IDSs. B-SIPS implementation correlates device power consumption with IEEE 802.11 and Bluetooth communication activity. Irregular and attack activity is detected and reported to the intrusion detection engine for correlation with existing signatures in a database and for forensic investigation by a security manager.**

***Index Terms*—Intrusion Detection, Battery, Wireless Security**

I. Introduction

This paper examines battery power constraints as a nontraditional intrusion detection method for Bluetooth and IEEE 802.11 (Wi-Fi) capable devices. This research will investigate and develop signatures for Bluetooth attacks, determine power traces over time as well as correlate some existing wireless network-based attacks as a proof-of-concept. The system employs the *Canary-Net* concept of using small mobile devices as early warning sensors in order to refine the resulting correlations of attack traces to improve the security administrator's view and to add forensic analysis tools for mining the system's online database for attack determination.

Once outside the cradle, battery power is a crucial resource. Much research over the last decade has been directed toward improving the performance, efficiency, and capability of small mobile computing devices; however, battery performance has only slightly improved in the same time span [1]. Conserving battery life is an important aspect of extending device usage. However, some researchers have suggested that battery life could be reduced to a quarter of its normal life if the device is kept under continual attack [2]. This research offers a viable model and working system for monitoring power demands that directly affect mobile hosts and can be used to detect attacks and other irregular communications activity. Using the *Battery-Sensing Intrusion Protection System* (B-SIPS), unusual power usage coupled with network traffic activity can be correlated amongst mobile client devices. This monitoring can lead to early warning and subsequent detection of new or previously *unsignatured* attacks.

In wired networks, intrusion detection analysts increasingly rely on layered defenses for attack detection and containment. Often, two or more traditional signature-based intrusion detection systems (IDSs) will be employed as will host-based IDS applications to monitor critical devices within the network sub-domain boundaries. Signature and anomaly-based IDS technologies provide the security administrator additional tools intended to detect and defeat adversarial activities that, once corrected, create greater system performance.

Di Pietro et al. suggested that the wireless environment will be dominated by handheld/wearable wireless (HWW) devices that will require frequent communication with other appliances which must remain transparent to the user [3]. The primary security weakness in the wireless environment is the fact that communications use radio signaling such that a knowledgeable attacker could monitor, capture, and potentially inject traffic, bypassing the traditional layered defenses without being observed. This creates a situation where each wireless-capable notebook computer, personal digital assistant (PDA), smart cellular phone, radio frequency identification (RFID) tag, and even wireless sensor device is its own first and last line of defense.

Anomaly detection systems (ADSs) comprise a wide variety of systems that seek to characterize network communications traffic and then deduce unusual activity from the norm [4] [5]. Many problems abound with profiling network traffic because networking environments always change. ADS technology, such as *StealthWatch+Therminator*, can provide real-time visualization of network traffic and pattern-less detection of known and unknown attacks against sensitive data as well as network assets [6]. Although ADSs show promise, they are often difficult to tune and monitor.

B-SIPS acts, in part, as an ADS by measuring power dissipation over time, which is compared against established host state thresholds to trigger anomalous activity alerts. These threshold breaches coupled with packet header data are then fed to an intrusion detection engine (IDE) for correlation. To establish a tripwire to alert the system, B-SIPS employs the

Tim Buennemeyer is a Ph.D. student in the Bradley Department of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University, Blacksburg, VA 22061 (e-mail: timb@vt.edu).

Dr. Grant Jacoby is a research scientist at United States Military Academy, West Point, NY 10996 (email: grant.jacoby@usma.edu)

Wayne Chiang is a senior student in the Computer Science Department at Virginia Polytechnic Institute and State University, Blacksburg, VA 22061 (e-mail: wchiang@vt.edu).

Randy Marchany is the Director of the Information Technology and Security Lab at Virginia Polytechnic Institute and State University, Blacksburg, VA 22061 (email: marchany@vt.edu).

Dr. Joe Tront is a member of the Bradley Department of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University, Blacksburg, VA 22061 (e-mail: jgtront@vt.edu).

1-4244-0130-5/06/$20.00 ©2006 IEEE

foundational power equations that simply state that energy is related to the position of an electric charge in an electric field. The electrical energy of a charge Q situated at the electric potential V is equal to the product QV. If V is a potential difference, the same expression gives the energy transformed when the charge moves through the potential difference, so electrical energy is the integral of the power over time:

$$W = \int_{t_1}^{t_2} p(t)\,dt = \int_{t_1}^{t_2} v(t)i(t)\,dt \quad (1)$$

p(t) is the instantaneous power, *v(t)* and *i(t)* are the voltage and current as a function of time, respectively. For direct current (DC), this simplifies to:

$$W = P \cdot (t_2 - t_1) = V \cdot I \cdot (t_2 - t_1) \quad (2)$$

With these fundamental energy equations providing the basis and initial functionalities of the detection system, B-SIPS examines instantaneous current changes, in milliamperes (mA), using a Dynamic Threshold Calculation (DTC) algorithm. The energy sampling and threshold calculations are taken every 500 milliseconds and then transmitted to a server. The goal of this system is to fill a perceived detection deficiency between traditional network and host-based IDSs and ADSs by using detected current above the DTC value as a tripwire to sense anomalous activity, power exhaustion, and other types of network attacks.

B-SIPS is a hybrid IDS that combines aspects of statistical anomaly detection with rules-based intrusion detection methods. B-SIPS serves to measure anomalous activity on the client device predicated on power constraints. Jacoby determined that using a battery-based IDS approach was feasible and further suggested that it is extraordinarily difficult for an attacker to manipulate an attack's energy and time without detection [7]. This observation that attacks can drain device battery power indicates a problem niche within both traditional signature-based IDS and ADS technologies that warrants further investigation.

Typically, rules-based IDSs and ADSs do not examine battery power changes, so this circumstance provides an opportunity window for B-SIPS to succeed and contribute to IDS research. By extending battery activity sensing, this research suggests that many existing and some unsignatured attacks can be detected using battery constraints and a threshold sensing methodology. This innovative, hybrid IDS technology coupled with the Canary-Net concept of employing HWW devices as sensors provides the security manager a robust and scalable detection mechanism with an integrated correlation capability using probabilistic bounds and measures to determine attack scope.

The rest of this paper is structured as follows. Section II presents background issues and related work. Section III discusses the Canary-Net concept of employing small mobile devices as intrusion sensors, the B-SIPS approach, methodology, and design issues. Section IV presents the innovations, testing, and initial analysis. Lastly, Section V provides a succinct conclusion and direction for future work.

II. Related Work

The security of power-constrained mobile hosts was generally considered as an afterthought compared to service availability. In the wireless realm, battery power is an important resource, especially for small, mobile devices that presents designers with a perplexing problem of choosing more security at the expense of more power usage and potentially less service availability. This is an unresolved tradeoff that continues to challenge network and system developers. Wireless networks are vulnerable to an interloper or eavesdropper who knows how to intercept the radio waves at the proper frequencies [7] [8]. Developing secure communication channels through proper authentication could increase service accessibility from a user's perspective but may further increase the device's computational and transmission requirements ultimately leading to faster battery power drain.

To better manage device power usage toward extending battery life, an Advanced Power Management (APM) technical specification was developed. APM provided a cooperative environment to conserve device power by turning off certain features of the computer such as the monitor, hard disk drives, and other computer peripherals when not in use [9]. APM is an Application Program Interface (API) which allowed computer and Basic Input Output System (BIOS) manufacturers to include power management into their BIOS and operating systems (OSs) that reduced power consumption. The next evolution in power management was the Advanced Configuration and Power Interface (ACPI) that established an industry-standard for interfaces to OS directed configuration and power management on laptops, desktops, and servers [10]. ACPI progressed the existing collection of power management BIOS code and APM application programming interfaces into a well-defined power management and configuration interface specification. The ACPI specification enabled new power management technology to evolve independently in OSs and hardware while ensuring that they continue to work together. The Smart Battery System Implementers Forum offered an open systems communication standard for industry-wide adoption that described data sharing directly between batteries and the devices they powered [11]. The goal was to improve battery efficiency and lifespan, and to expand interoperability between products from battery, software, semiconductor, and system vendors [7] [11]. Their introduction of a Smart Battery Data (SBData) specification was used to monitor rechargeable battery packs and to report information to the System Management Bus (SMBus), which implemented a two-wire bus design that could communicate battery data directly to the device [12].

Without these technological advances in ACPI and smart batteries, developing battery constraint-based intrusion detection and this Canary-Net and B-SIPS research endeavor would not be feasible. As noted above, interoperability and low power design was inspired by the demand to significantly increase battery life and thus the usefulness of small mobile

hosts. Minimizing power consumption is paramount. With the introduction of smart battery technology, the battery pack's embedded electronics can hold SBData, measure battery operating parameters, calculate and predict battery performance, control battery charging algorithms, and communicate with other SMBus devices [13]. Interestingly, the smart battery concept was motivated by the idea that the rechargeable battery would manage its own charging.

Other researchers have investigated extensions to these standard conventions. Benini et al. introduced Dynamic Power Management (DPM) to account for battery constraints [14] [15]. Its goal was to optimize battery subsystem scheduling and management to better satisfy device power requirements, but it failed to address overall consumption.

As the scope of IDS knowledge continually expands and matures in the wired world, certain aspects permeate into the wireless domain. Cannady suggested that IDSs be employed together to form a layered defensive approach and that those systems need to use various algorithms to detect security violations, which include algorithms and methods for statistical-anomaly detection, rules-based detection, and hybrids of the two [16].

Nash and Martin et al. developed a battery constraints-based IDS for laptop computers toward defending the system against various classes of "battery exhaustion attacks" of their own design [17]. They leveraged the laptop's robust computational power to estimate power consumption of the overall system based on metrics which included CPU load, disk read and write access, and network transmissions and receptions by using a multiple linear regression model. This data was combined with performance data counters in the Windows NT OS environment. Using multiple linear regressions allowed them to find the correlation of coefficients for each of the measured metrics and a way to determine component power usage from the overall device's power consumption. Moreover, they adapted this concept of estimating system-wide power consumption on a per process basis as a method for indicating possible intrusion and identifying rogue processes on mobile devices. As with any trigger-based system, the challenge is in determining the proper thresholds. Unauthorized activity that falls below the settings may go undetected.

Jacoby developed a *Battery-Based Intrusion Detection* (B-BID) approach as a purely host-centric IDS solution for mobile handheld devices [7] [8]. This system was comprised of three distinctive IDS applications based on the power capabilities of the device regarding resources and processor clock speeds. At the low power end (fewer resources and slower clock speeds) was the *Host Intrusion Detection Engine* (HIDE), which was a rules-based program tuned to determine battery behavior abnormalities based on threshold levels. In the mid range, a complementary module called the *Source Port Intrusion Engine* (SPIE) was employed to capture network packet information, during a suspected attack. At the high end, the *Host Analysis Signature Trace Engine* (HASTE) was used to capture and correlate signature patterns using periodogram analysis in the frequency domain to determine the dominant frequency and magnitude (x,y) pairs. To our knowledge, this system presented the first feasible working IDS solution for a small mobile host using battery constraints. However, its deficiency was that it allowed the device user the option to monitor the system automatically or to manually invoke actions to impede an attack. Although the manual approach is possible, it is unlikely that the device user would monitor the host continuously and be able to respond fast enough to prevent substantial power depletion on a regular basis. As a concept, the B-BID approach presents fertile ground for further development, scalability, and research extension.

With any attack, above normal power consumption by the device is likely. If a small mobile device is kept in a higher activity state for extended periods of time, then the battery power will be depleted much faster than normal, decreasing its expected life. Stajano and Anderson suggested the idea of energy depletion attacks as early as 1999, which they described as "sleep deprivation torture" [18]. An emerging class of attacks, *battery exhaustion* and *denial of sleep* attacks represent malicious situations whereby the device's battery has been unknowingly discharged, and thus the user is deprived access to information [2] [19]. Since system designers of power constrained devices incorporate power management to monitor active processes and to shutdown unnecessary components, sleep deprivation and power exhaustion attacks seek to invade and exploit the power management system to inhibit the device's ability to shift into reduced power states.

In analyzing battery attacks against laptop computers, Martin and Hsaio et al. further subdivided sleep deprivation attacks into three basic categories: service requesting, benign, and malignant power attacks [2]. A *service requesting power attack* attempts to repeatedly connect to the mobile device with genuine service requests with the intent of draining power from the device's battery. A *benign power attack* attempts to start a power demanding process or component operation on the host to rapidly drain its battery. A *malignant power attack* actually succeeds at infiltrating the host and changes programs to quickly devour much more power than is typically required.

An attack of this nature will use more power, and thus demonstrates the need for an integrated battery-sensing IDS. B-SIPS research is developing an innovative battery power constraint-based model and system to help defend small mobile computers, smart cellular phones, and communication enhanced PDAs. B-SIPS provides threshold monitoring and alert notification as a host application, which alerts on power changes detected on small wireless devices. These hosts are employed as sensors in a wireless network and form the basis of the *Canary-Net* IDS. This detection capability is scalable and complementary with existing commercial and open system network IDSs. B-SIPS implementation correlates device power consumption with WiFi, Bluetooth, and in the future for cellular phone communication activity. Irregular

and attack activity is detected and reported to the online IDE server for comparisons against attack trace signatures. In the future, intrusion detection tools must also perform correlation between hosts and robust network-based IDSs.

III. Methodology and System Design

This research offers a viable model and working system for monitoring power demands that directly affect mobile hosts and can be used to detect attacks and other irregular communications activity. Using B-SIPS, unusual power usage coupled with network traffic activity can be correlated amongst mobile client devices. This monitoring can lead to early warning and subsequent detection of new or previously unsignatured attacks.

A. IDS Algorithms--A Primer to Attack Discovery

Statistical-anomaly detection methods attempt to detect attacks by characterization and analysis of audit logs and a system's behavior, establishing a baseline profile of perceived normal system activity. Any activity outside these established system profile norms, such as threshold breaches, is considered to be an intrusion until proven otherwise through forensic analysis. Systems employing statistical-anomaly detection are beneficial because they can detect novel and zero-day attacks without prior knowledge. However their main drawback is that anomaly detection can generate numerous false positives, which wastes valuable security administrator investigation time. Ultimately, administrator experience with the system determines how effective anomaly detection is at finding malicious events. B-SIPS detects anomalous activity that exceeds the system's dynamic threshold value. The DTC algorithm iteratively considers known device processes, backlighting, and system states. Although false positives are always a possibility with any detection system, B-SIPS is less prone to false positive alerts because the DTC considers normal device power draining activities and then only triggers an alert when the threshold is exceeded by the device's response to anomalous activity. A tangible goal of B-SIPS is to save valuable security administrator time by reducing false positive alert investigations.

Rules-based detection methods, such as "if-then" constructs, employ signatures to characterize and identify known attacks. Aspects of packet traffic, unique data patterns, and specific audit log entries all provide valuable clues and are often employed in rules-based signature development. Signature profiles are updated regularly as attacks emerge and are identified, so security administrators have to habitually maintain their system's signature base. Rules-based IDSs are a mainstay in today's network defenses, and they provide a valuable capability because they consistently detect most known attacks with relatively few false positives.

B. A Hybrid Approach: B-SIPS

B-SIPS is a hybrid of ADS and traditional IDS because it triggers on energy draining events that were not expected using statistical bounds to assess an attack. It also attempts to match power traces of some known attacks and then correlate the attack with other network IDSs. As a hybrid of ADS and IDS, the goal of B-SIPS is to rapidly detect power consumption changes in mobile hosts, which could indicate a possible attack and alert the user and security administrator of potential malicious activity such as denial of service (DoS), flooding attacks, viruses, and worms. B-SIPS addresses the hybrid IDS requirements by observing host device battery activity in Busy and Idle states. In the Suspend state, there is no way to measure activity. However, it is possible to measure the number of times a device enters the Suspend state. An attacker, potentially trying to fool the system to subvert the threshold, could use this state changing situation as an attack vector [7].

Because B-SIPS detection capability focuses on small mobile hosts that are Bluetooth and WiFi enabled, conservation of power is of paramount consideration in determining what information is captured, where the information is stored, when the attack signatures (if available) are transmitted, and how intrusion correlation is conducted. B-SIPS alert notification is done at the client for the user and across the network at the CIDE server for the security administrator in the system. Certain power-depleting attacks such synfloods, ping floods, smurf attacks, some buffer overflows, and various DoS can be profiled by their pulsing pattern or continuous high drain characteristics, while other attacks merely create temporary spikes in power usage and are much more difficult to pattern. Ultimately, a hybrid IDS such as B-SIPS needs to capitalize on the advantages of rules-based approaches to minimize false positives and detect known attacks. Where possible, B-SIPS should detect novel attacks like an ADS without generating false positives that waste security administrator time.

As low powered devices attempt to manage power consumption based on device needs, they regularly attempt to transition to a lesser state of power usage such as the Suspend and Sleep states. If elevated activity continues and power thresholds in Busy or Idle state are broken, then the system begins a chain of user and security administrator alerts. The user can take certain external actions to B-SIPS such as turning off an identified rogue process in MS Mobile 5.0, turning off *flight mode*, and starting antivirus software. Most users of computer systems have only limited knowledge to accomplish defensive measures, so B-SIPS attempts to rapidly push the detected attack information upstream to the *Correlation Intrusion Detection Engine* (CIDE).

The CIDE attempts to match known power depletion attack signatures to notify the security administrator in near real-time that an attack has occurred or may be ongoing. The system can detect attacks, transmit the threshold breach data, and receive an alert within five seconds. This round trip alert time can be negatively affected by flooding and DoS attacks, but B-SIPS is still able to respond. Breaches of thresholds in power usage data are captured and paired with inbound packet header information and then passed to the CIDE. This trace

data is then correlated with other network IDS information and then matching activity attempts to minimize forensic analysis time and effort to expedite the security administrator's ability to effectively respond to the threat. If no match is found in the signature base, then the activity could indicate an unsignatured attack. The final system component is the active involvement of the security administrator or, in the future, other upstream intrusion protection systems that can invoke further defensive measures to impede attacks.

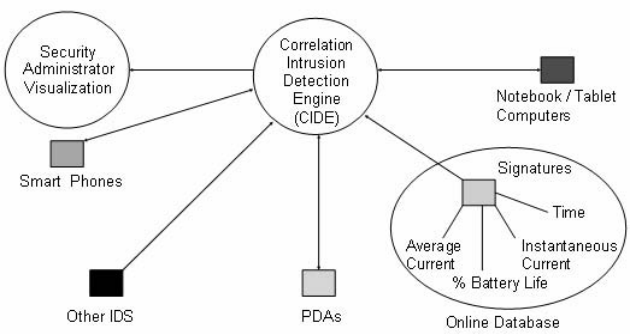


Fig. 1. Canary-Net conceptualization.

The Canary-Net (see Fig. 1) concept considers the nature of virulent self-spreading worms, botnets, and attacks that seek to compromise numerous devices in a network. As a scalable aspect of B-SIPS, Canary-Net's goal is to integrate intrusion detection onto small mobile hosts on the network and provide a common methodology of providing additional defensive and alert correlation measures. The idea is that all the mobile devices, termed "canaries" which represent birds that are very sensitive to changes in the environment, will act as IDS sensors, using B-SIPS. If a spreading attack occurs that affects the small mobile hosts, these sensors would provide multiple alerts to the administrator that would otherwise go undetected by the security administrator until after irreparable damage may have already occurred.

C. Power Depletion Signatures

The majority of prevalent attacks are annually identified and categorized by the SANS Institute and the US CERT/CC, which allow an opportunity to create relevant power-based trace signatures that complement and support the identification of many attacks [20] [21]. Additionally, Jacoby created approximately a dozen device specific power depletion attack signatures which are usable in this system [8]. Initially, B-SIPS focuses on existing network-based attack signatures because of available signatures and the opportunity to correlate attacks with other existing network IDSs such as *Snort* [22]. These attack signatures are most viable if they have a high energy drain potential such as a DoS or if they present timing patterns in their attack or infection mode.

The changing state of attack vectors has opened another avenue for attack signature development, which encompasses characterization of some Bluetooth wireless personal area network (WPAN) attacks. Applying this methodology may be useful in discovering recent attacks such as the *Cabir* virus and its many variants in mobile devices which use the Symbian OS on Series 60 cellular phones, MS CE, and MAC OSX Bluetooth environments [23]. In the future, Bluetooth attacks will be more prevalent as flaws are discovered and then exploited, which will offer greater opportunities to develop power-based traces since most Bluetooth capable devices tend to be of low powered design. Attacking exposed hosts through unsecured WPANs would allow the attacker direct access to the mobile device and its OS environment, completely bypassing any upstream defensive measures. This observation suggests that small mobile hosts have an increasing need for hybrid IDS protection such as B-SIPS.

D. B-SIPS Design

The B-SIPS design is software-based and focuses on providing an early warning capability for the small mobile host. Like HIDE, B-SIPS attempts to detect power usage threshold violations in Idle and Busy states. The idea is that normal power usage in each state can be determined to set a threshold accordingly. Excessive activity, above the modeled threshold, can cause a violation to be reported. Repeated threshold violations will be measured and associated with network packet header information. Security specialists consider network attacks against PDAs likely, so this research intends to use packet header data as a means to correlate anomalous activity with actual attacks. This combined threshold violation and packet header information is transmitted back to the CIDE for trace signature matching and correlation with other relevant IDS information such as *Snort*, firewall, or router logs. Because B-SIPS runs on low powered mobile hosts, an essential requirement is that the software must run as a background process and not use a significant amount of device power while in monitoring mode.

In the initialization and monitoring phase, battery temperature is assessed and compared against the normal operating range for the battery type. This phase of detection is accomplished by the battery power sensing module, which is illustrated in Fig. 2. Next, baseline DTC power usage estimates are compared to actual device power usage. Depending on the device's battery state, higher power usage thresholds are established for Busy and Idle. Network activity is monitored but not logged in conjunction with the battery discharge rate. Once B-SIPS detects a potential attack in terms of a power usage threshold violation, active logging is invoked to quickly connect anomalous power usage with unexpected network traffic. These actions provide the user with an alert to take precautionary actions such as stopping an unfamiliar process, starting an antivirus package, or disconnecting from the network temporarily.

The capturing process begins the trace signature characterization method, which is used upstream by both the CIDE to match and create signatures in Fig. 2 and by the security administrator to identify malicious system-wide activity and begin active intrusion protection measures. CIDE requests known signatures from the online database and attempts to make matches of various attacks while alerting the user and security administrator of the problem. If no known

attack is matched, then a "no match" alert is sent. This is an indication of possible malicious activity, unexpected network traffic, or system configuration problems but, it could well indicate that a new or unsignatured attack is ongoing against B-SIPS devices.

Because B-SIPS uses battery constraints and current thresholds to trigger device alerts in Idle and Busy states, the generation of false positives and false negatives is of great concern. Any intrusions that are missed are labeled *false negatives*. When normal data activities are misidentified as attacks, they are labeled *false positives*. Like SPIE, B-SIPS attempts to minimize both false positives and false negative through dynamic threshold tuning and by capturing events and pairing that data with traffic header information. Although unlikely, an attacker with B-SIPS knowledge could potentially trigger a long series of false negatives to intentionally cause power exhaustion on the device.

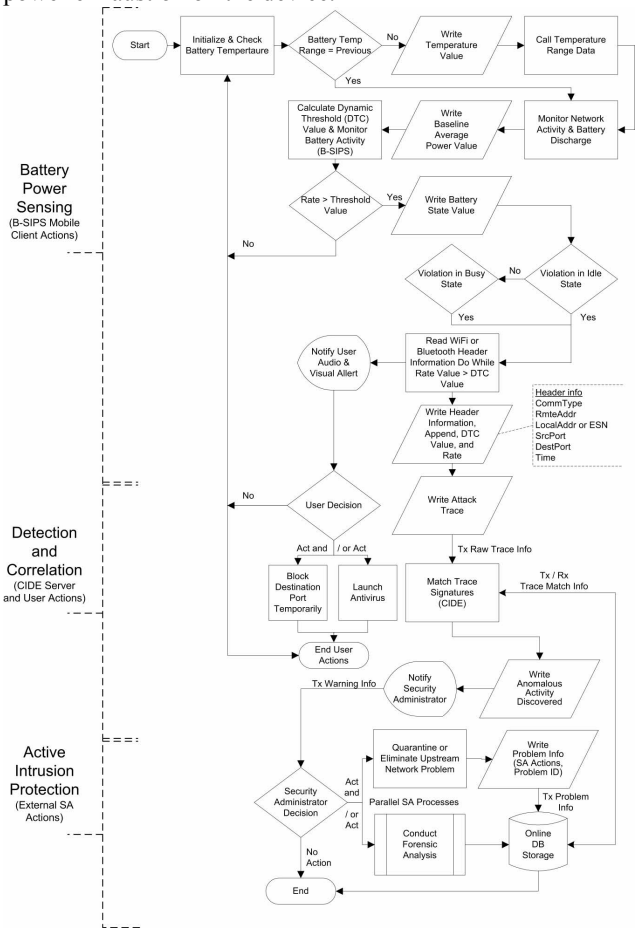


Fig. 2. B-SIPS information flowchart and design adapted from [7] [8].

The last component of B-SIPS is the active intrusion protection shown in Fig. 2 whereby the security administrator has external options to consider and invoke to further protect the afflicted devices. Active intrusion protection complements layered defensive approaches and provides notifications and alerts directly to the administrator to bring attention to anomalous activity that occurs on the mobile host. Once alerted by B-SIPS that unexpected power depletion activity has occurred, the user, as well as the security administrator, can then take appropriate actions to protect the host. These actions range from starting an antivirus package, turning off processes, or running other more robust defensive software. This phase also provides necessary feedback in terms of intrusion signatures that are posted in an online database for further examination by skilled security specialists. The B-SIPS design considers attack, detection, and proliferation issues upfront and attempts to connect the threshold data with packet header information to expedite the administrator's searching and analysis process. However, it is possible that attacks may exhibit very low power usage and not exceed the DTC on every device. By using the Canary-Net concept, it is possible that those attacks could breach the thresholds of other devices and then be detected. This is further supported by the Canary-Net concept, which employs B-SIPS enabled PDAs as sensors within the wireless environment. Often, attackers will follow the "island hopping campaign" method, which they use to grab as many devices in as rapid a time as possible. Using correlated B-SIPS reports, the security administrator can quickly determine the devices under attack, follow the attacker's trail, and then take corrective measures.

E. B-SIPS Developmental Environment

The B-SIPS suite of tools is initially produced for Dell Axim X51v PDAs running Microsoft Mobile 5.0 OS as well as the Dell Axim X30v running Pocket PC 2003. B-SIPS is crafted using C# Visual Studio.Net 2005 with the .NET Compact Framework. The clear benefit is the ability to program in various environments, incorporate the ACPI members and function calls, and then convert them into C# using the built-in PDA emulator. This capability allows for rapid application development and testing.

IV. Testing and Initial Analysis

Preliminary B-SIPS testing demonstrated that the battery sensing capability function could capture the power drain of two PDAs simultaneously. This test used the *hping2* packet crafting tool to generate synflood and ping flooding attacks. The B-SIPS client in Fig. 3 transmitted the threshold breaches to the server-based CIDE using UDP packets to minimize communication traffic overhead. The attack detection shown in Fig. 4 indicates a PDA's Idle state threshold was violated.

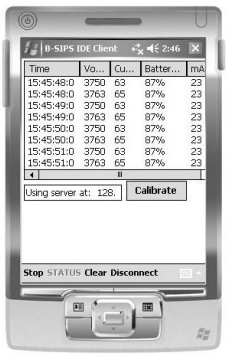


Fig. 3. B-SIPS client monitoring of normal activity.

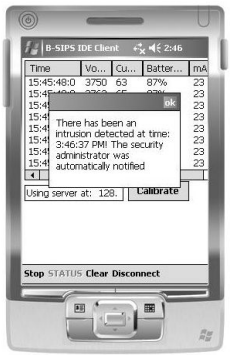


Fig. 4. B-SIPS report of Idle state threshold breach.

B-SIPS calculates the DTC value every 500 milliseconds for comparison with the instantaneous current. When a threshold breach occurs, B-SIPS transmits its reports to the CIDE server. The reporting continues while the DTC value is exceeded. Although rapid reporting has a strong potential benefit for early detection and corrective actions by the security administrator, there is a clear tradeoff in that the client device will expend additional energy to transmit a potentially high volume of reports which could lessen the useful battery life of the device. These tradeoffs still need to be measured and characterized, but it is believed that the benefits of constantly pulling reports for rapid notification will outweigh the power expenditure.

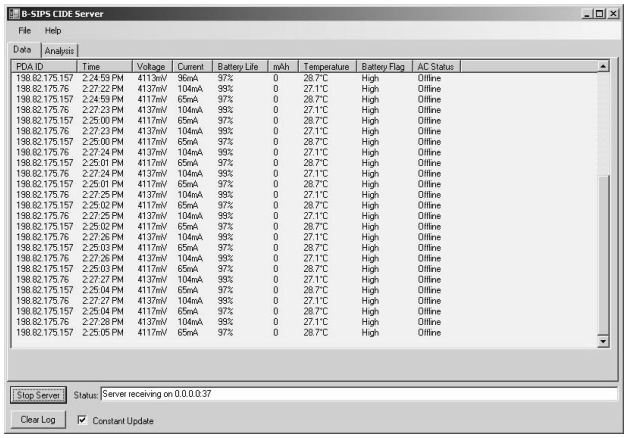


Fig. 5. Data reports of two B-SIPS enabled PDAs displayed on CIDE.

In Fig. 5, the transmitted PDA reports are assessed by CIDE. The correlation algorithm then compares the attack trace against a signature base and graphically represents the increased PDA power drain to alert the security administrator, which is displayed as a spike in near real-time on the security manager's console in Fig. 6. These captures are shown in continuous mode. Using *hping2* the attacks launched unexpected packets with no payload at the PDA, but an attack could have been easily executed using any readily available online attack crafting package such as www.metasploit.com to deliver a payload. With good results from B-SIPS for detecting a flooding style attack, the challenge will be to identify viable power-based profile traces for other network and Bluetooth attacks.

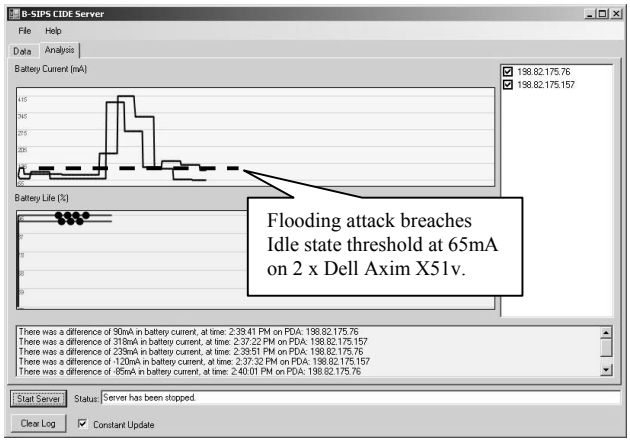


Fig. 6. Graphical view of battery depletion attack launched using hping2.

Lastly, the security administrator can further investigate the unusual activity by conducting a rapid forensic analysis in Fig. 7. The CIDE view provides some basic data mining tools, which show connections between suspicious activities associated to captured packet header information such as:

- Communication Type
- Remote Address
- Local Address (or ESN with cellular devices)
- Source Port
- Destination Port
- Time

Collectively, these datasets can be associated with an anomalous activity to help identify commonalities within and between end unit hosts.

Ultimately, the rapid response by the security administrator will be the critical enabler of B-SIPS. As with most IDSs, the primary challenge is correlating the activity to determine the event cause. This challenge is not trivial with large scale deployments, so B-SIPS seeks to complement those systems by providing early warning, activity correlation, and a forensic analysis tool set to assist in the investigative process.

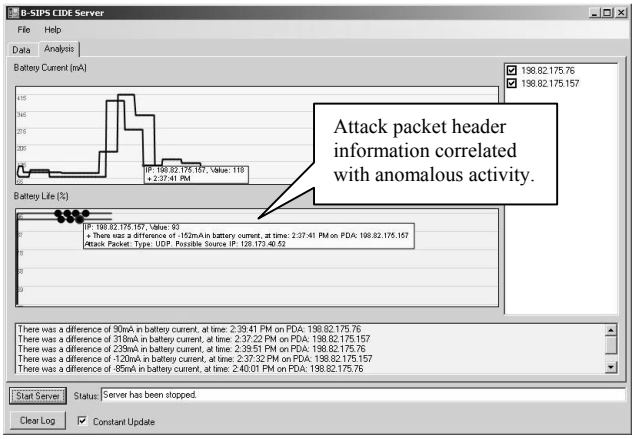
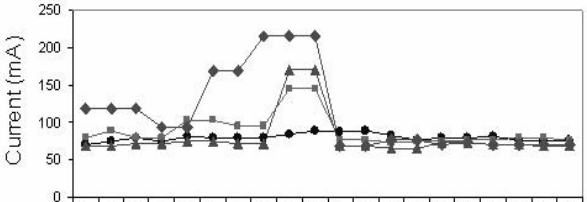


Fig. 7. Forensic analysis of attack; B-SIPS mouse-over capability shows attack vector with highlighted details.

The initial results show great promise that B-SIPS deployment is feasible as a tool for detecting unusual activity on small mobile hosts during periods of high power consumption. Of concern is the fact that B-SIPS operation on PDAs does come at a price, so some power must be expended to have some level of protection. Based on related research by [8], it is anticipated that B-SIPS will consume roughly 6% power under normal usage with no attacks and it should save approximately 10% power when the device is under attack.

Analyzing these initial results from the different types of attacks against B-SIPS, it can be readily observed that some attacks produced power consumption threshold breaches while the Dell Axim was in the Idle state. The first test employed a continuous ping to simulate network traffic. The purpose of this test was to produce conditions of high volume wireless network activity. The results produced from this test had no

profound impact on battery consumption. However, when the B-SIPS agent was attacked using DoS and flooding variants, it was able to detect irregular activity with the instantaneous current. When a synflood was initialized, the battery current would increase considerably for the period of the attack in Fig. 8. While this may seem significant, the most substantial effects were seen with a ping flood. In this attack, battery current would sharply increase, more than the previous synflood. It is notable that this surge in battery current lasted for a short period of time and then ended abruptly. Lastly, a combined attack created the largest drain in battery current, along with the greatest duration of time of these experiments. In this attack, the battery current shows a distinct range of values. This data can be used to develop power depletion attack traces for analysis and preventing attacks.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Regular Ping	71	75	79	75	81	79	79	79	85	89	87	89	83	76	79	80	81	76	75	77
Syn Flood	79	89	80	80	103	103	95	95	146	146	76	76	73	75	75	77	77	79	79	76
Ping Flood	68	68	72	72	75	75	72	72	171	171	68	68	66	66	74	74	70	70	68	68
Multiple Attack	118	118	118	94	94	168	168	216	216	216	69	69	76	76	71	73	71	71	71	71

Fig. 8. B-SIPS attack and response analysis.

V. Conclusion and Future Work

The concept of employing battery constraints as a means of intrusion detection is a new capability that was only recently made possible by developments in smart battery and advanced power management technologies. The prototypical B-SIPS design offers a hybrid intrusion detection method that can serve to protect small mobile computers from anomalous activity that seek to drain battery power excessively. This research asserts that small mobile hosts can be protected by B-SIPS, which triggers alerts based on power utilization threshold breaches. The next step of B-SIPS research will investigate and develop signatures for Bluetooth attacks, signature and correlate some existing wireless network-based attacks, explore the Canary-Net concept of early warning, and then refine the security administrator's view and forensic analysis tool set for mining the system's database.

References

[1] D. Siewiorek, "Energy locality: processing / communication / interface tradeoffs to optimize energy in mobile systems," Proceedings of IEEE Computer Society Workshop on VLSI 2001. Emerging Technologies for VLSI Systems. Orlando, FL, 2001.

[2] T. Martin, M. Hsiao, H. Dong, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," presented at Second IEEE Annual Conference on Pervasive Computing and Communications. Orlando, FL, 2004.

[3] R. Di Pietro and L. V. Mancini, "Security and privacy issues of handheld and wearable wireless devices," *Communications of the ACM*, vol. 46, pp. 74-9, 2003.

[4] R. Chinchani, S. Upadhyaya, and K. Kwiat, "Towards the scalable implementation of a user level anomaly detection system," presented at Military Communications Conference (MILCOM 2002). Anaheim, CA, 2002.

[5] M. F. Pasha, R. Budiarto, and M. Syukur, "Connectionist model for distributed adaptive network anomaly detection system," presented at International Conference on Machine Learning and Cybernetics. Guangzhou, China, 2005.

[6] M. Martin,"Therminator may squelch net attacks," www.newsfactor.com/perl/story/22383.html, 2003.

[7] G. A. Jacoby, R. Marchany, and N. J. Davis, "Battery-based intrusion detection a first line of defense," presented at the Fifth Annual IEEE SMC Information Assurance Workshop. West Point, NY, 2004.

[8] G. A. Jacoby and N. J. Davis, "Battery-based intrusion detection," presented at IEEE Global Telecommunications Conference (GLOBECOM 2004). Dallas, TX, 2004.

[9] Microsoft,"Advanced power management v1.2," www.microsoft.com/whdc/archive/amp_12.mspx, 2001.

[10] Advanced Configuration & Power Interface, www.acpi.info, 2005.

[11] Smart Battery System Forum, www.sbs-forum.org, 2005.

[12] System Management Bus, www.smbus.org, 2005.

[13] E. Thompson,"Smart batteries to the rescue," 2000.

[14] L. Benini, G. Castelli, A. Macii, and R. Scarsi, "Battery-driven dynamic power management," *IEEE Design & Test of Computers*, vol. 18, pp. 53-60, 2001.

[15] L. Benini, G. Castelli, A. Macii, E. Macii, M. Poncino, and R. Scarsi, "Extending lifetime of portable systems by battery scheduling," Proceedings of Design, Automation and Test in Europe Conference and Exhibition 2001. Munich, Germany, 2001.

[16] J. Cannady and J. Harrel, "A comparative analysis of current intrusion detection technologies," Proceedings of Technology in Information Security Conference. 1996.

[17] D. C. Nash, T. L. Martin, D. S. Ha, and M. S. Hsiao, "Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices," presented at Third IEEE International Conference on Pervasive Computing And Communications Workshops. PerCom 2005 Workshops. Kauai Island, HI, 2005.

[18] F. Stajano and R. Anderson, "The resurrecting duckling: security issues for ad-hoc wireless networks," Proceedings of 7th International Workshop on Security Protocols, Cambridge, UK, 1999.

[19] M. Brownfield, G. Yatharth, and N. Davis, "Wireless sensor network denial of sleep attack," presented at the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop. West Point, NY, 2005.

[20] SANS, "The twenty most critical internet security vulnerabilities," www.sans.org/top20/, 2005.

[21] US-CERT, "US-CERT vulnerability notes database," www.kb.cert.org/vuls, 2006.

[22] Snort.Org Forum, www.snort.org/reg-bin/ forums.cgi.

[23] Symantec, "SymbOS.Cabir," http://securityresponse.symantec.com/avcenter/venc/data/symbos.cabir.html, 2004.