Battery Exhaustion Attack Detection with Small Handheld Mobile Computers

Timothy K. Buennemeyer, Michael Gora, Randy C. Marchany, and Joseph G. Tront
Bradley Department of Electrical and Computer Engineering
Virginia Polytechnic Institute and State University
Blacksburg, Virginia
{timb, gora, marchany, jgtront}@vt.edu

Abstract*—This paper describes a unique Battery-Sensing Intrusion Protection System (B-SIPS) for mobile computers, which alerts on power changes detected on small wireless devices, using an innovative Dynamic Threshold Calculation algorithm. B-SIPS enabled hosts are employed as sensors in a wireless network and form the basis of the intrusion detection system (IDS). B-SIPS implementation correlates device power consumption with IEEE 802.11 Wi-Fi and 802.15.1 Bluetooth communication activity. This battery exhaustion, Wi-Fi, and Bluetooth attack detection capability is scalable and complementary with existing commercial and open system network IDSs. Irregular and attack activity is detected and reported to an intrusion detection engine for correlation with existing trace signatures in a database and for forensic investigation by a security manager.

Keywords-intrusion detection, battery, wireless security

I. INTRODUCTION

The primary challenges in developing defensive applications such as intrusion detection systems (IDSs) for small, wireless computers are limited processing capability, memory, and battery resources. Traditionally, network and host-based IDSs employ rules to detect known malicious activity. Anomaly detection systems (ADSs) use statistical methods to establish a system profile and then trigger alerts when that normal profile is violated. This research initiative is developing a battery-based detection system that employs mobile devices as sensors that use an instantaneous current-based threshold algorithm to indicate anomalous activity and trigger alerts.

An indicator that a rogue process is being run on a device without the knowledge of the user is an unexplained increase in the instantaneous current drawn from a device's battery. This could indicate anomalous activity such as a worm spread, virus infection, network probing, flooding, or denial of service (DoS) attack. All of these malicious activities can cause the battery current to rise such that a well-designed system could detect the illicit activity. The *Battery-Sensing Intrusion Protection System* (B-SIPS) detection capability provides security administrators (SAs) with a complementary tool in a network environment as a nontraditional method to detect anomalous battery exhaustion, IEEE 802.11 (Wi-Fi), and IEEE 802.15.1 (Bluetooth) attack activity that standard IDSs are incapable of detecting [1].

The rest of this paper is structured as follows. Section II presents related work. Section III discusses the exhaustion attacks effects, the system design, and the algorithmic approach to B-SIPS. Section IV presents the testing and analysis of various attacks against small mobile computers. Section V provides a conclusion and direction for future work.

II. RELATED WORK AND BATTERY EXHAUSTION ATTACKS

The security of power-constrained mobile hosts is generally considered as an afterthought in comparison to service availability. Battery power is an important resource in the wireless domain, especially for small, mobile devices. This presents designers with the perplexing problem of choosing more security at the expense of greater power usage and potentially less service availability. This is an unresolved tradeoff that continues to challenge network and system developers. Establishing 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, leading to faster battery drain.

An Advanced Power Management (APM) technical specification was developed to better manage device power usage to extend battery life [2]. APM is an application programming interface which allowed computer and Basic Input Output System (BIOS) manufacturers to include power management into their BIOS and operating systems (OSs), thus reducing energy 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 [3]. The ACPI specification enabled 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 [4]. 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

1-4244-1039-8/07/$25.00 ©2007 IEEE

bus design to communicate battery data directly to the device [5] [6].

Stajano and Anderson [7] suggested the idea of energy depletion attacks as early as 1999, which they described as *sleep deprivation torture*. 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 [8] [9]. Since system designers of energy-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 et al. [8] further subdivided sleep deprivation attacks into three basic categories: service-requesting, benign, and malignant power attacks. 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 successfully infiltrates the host and changes programs to devour much more power than is typically required.

As mobile computers become more widely adopted and deployed, they become viable targets for attackers. Racic et al. [10] demonstrated successful battery exhaustion attacks that transited commercial cellular phone networks to exploit vulnerabilities in an insecure multimedia messaging service, context retention in the packet data protocol, and the paging channel. These and other attacks could drain the battery power of target devices and render them useless in a short period of time by keeping them in a busy state. Most concerning is the fact that the cellular phone user and network administrator were unaware that the attack was ongoing. An attack of this nature will use more device power, and thus demonstrates the potential effectiveness of 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 Personal Digital Assistants (PDAs). Interoperability and low power design were inspired by the demand to significantly increase battery life and thus the usefulness of small mobile hosts. Battery constraint-based intrusion detection and this B-SIPS research endeavor would not be feasible without these technological advances in ACPI and smart batteries.

III. B-SIPS DESIGN

When a small mobile device is kept in a high activity state for extended periods of time, the battery power is depleted faster than normal, decreasing its expected charge life. This research seeks to protect the device's battery life by detecting anomalous battery draining activities. The B-SIPS provides threshold monitoring and alert notification as a host application, which triggers during detected power changes on small wireless devices. These hosts are employed as sensors in a wireless network and form the basis of the *Canary-Net* IDS [11]. This detection capability is scalable and designed to complement existing commercial and open system network IDSs. B-SIPS correlates device power consumption with Wi-Fi and Bluetooth communication activity. Irregular and attack activity is detected and reported to the server for comparisons against attack trace signatures.

The system was developed in Microsoft C# in the .NET Compact Embedded (CE) environment [12]. The client code was ported to run within Windows CE for Mobile 5.0, and the B-SIPS suite of tools is produced for Dell Axim X51v PDAs running Mobile 5.0 as well as the Axim X50v, Axim X30, and HP 4155 running Pocket PC. The detection tools were employed on Cingular 8125 and Samsung i730 smart phones operating with Mobile 5.0 Phone as well.

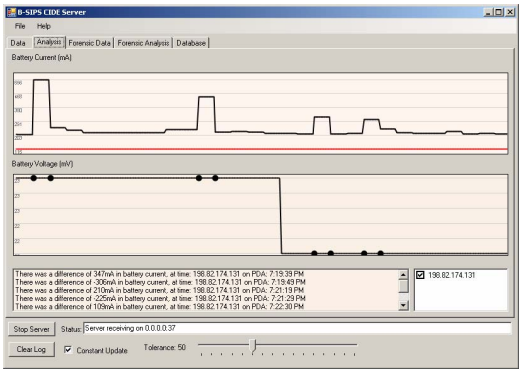
B-SIPS is a hybrid of ADSs and traditional IDSs because it triggers on unexpected energy draining events using statistical bounds to assess an attack. It also attempts to match power traces of some known attacks and then correlate the attack with other network IDSs. The goal of B-SIPS is to rapidly detect power consumption changes in mobile hosts, which could indicate a possible attack, and alert the user and SA of potential malicious activity.

B-SIPS detection capability focuses on small mobile hosts that are Bluetooth and Wi-Fi enabled, so conservation of power is of paramount consideration in determining what information is captured, where the information is stored, when the attack signatures are transmitted, and how intrusion correlation is conducted. B-SIPS alert notification is done on the client device for the user and across the network by a server for the SA. Certain power-depleting attacks such as floods, buffer overflows, and various DoS attacks 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.

B-SIPS uses battery constraints and current thresholds to trigger device alerts in Idle and Busy states. The potential for false positives and false negatives is of great concern. B-SIPS strives to minimize both false positives and false negatives through dynamic threshold tuning. Also, the system attempts to correlate alerts with packet header information for forensic analysis. B-SIPS detects anomalous activity that exceeds the system's dynamic threshold value. The Dynamic Threshold Calculation (DTC) algorithm iteratively considers known device processes, backlighting, and system states [1]. Although false positives are 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.

B-SIPS calculates the DTC value as backlight setting, process, and state changes occur within the device for comparison with the instantaneous current reading. However, the smart battery only provides the instantaneous current reading once per second due to limitations in the smart battery chipset. When a threshold breach occurs as shown in Fig. 1,

Fig. 1. B-SIPS client alert.



nmap SYN: -sS, UDP: -sU, Xmas: -sX, FIN: -sF

Fig. 2. Invasive scan detections on Axim X51v.

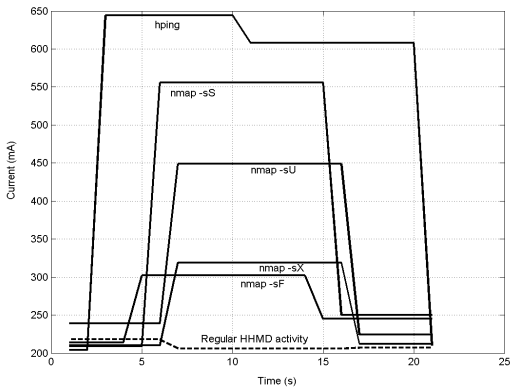


Fig. 3. Battery power attack contrasts.

B-SIPS transmits its reports. 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 SA, there is a clear tradeoff in that the client device will expend additional energy to transmit a potentially high volume of reports. This could reduce the useful battery life of the device. It is believed that the benefits of pulling reports each second for rapid notification outweigh the power expenditure.

The transmitted PDA reports are assessed by the server, using a correlation algorithm. The attack trace is compared against a signature base and the increased PDA energy drain is graphically represented to alert the SA. It is displayed as a spike in near real-time on the SA's console, depicted in Fig. 2.

Using *nmap* and *hping2* tools to attack an Axim X51v, the device's battery power drain is contrasted in Fig. 3. These attack tools launched packets with no payload at the PDA, but an attack could have been executed using any readily available online attack crafting package to deliver a payload.

IV. Testing and Analysis

The experiment setup employs a 1Ω precision resistor that is placed in series between the PDA and its smart battery. By using the known 1Ω resistance with Ohm's Law (I=V/R), the instantaneous current being used by the device is determined by measuring the voltage drop across the resistor. A Tektronix TDS694C 3GHz real-time digital oscilloscope was used to record these voltage changes. A 1Ω resistor, while causing minimal interference with the device, does not provide a large enough voltage drop to be accurately measured. Therefore, an amplification circuit was modified from examples [9] [13] [14] to allow for a more robust signal and is shown in Fig. 4.

An EXTech 382213 12V regulated DC power supply is used to drive the amplification circuit. The amplification circuit is connected in parallel with the 1Ω resistor and in turn provides an amplified voltage reading to the oscilloscope. The gain is determined by the resistor used on the two Rga pins in Fig. 4. In this situation a 10MΩ resistor was used, resulting in a gain of 5 as determined by the INA2126P amplifier's documented gain formula (G = 5 + 80KΩ/Rga). This low gain produced measurable output while maintaining the highest possible signal fidelity for this amplifier. This arrangement samples the PDA's battery drain response to Wi-Fi and Bluetooth attacks.

The resulting waveform is sampled by an oscilloscope, and the raw amplitudes, as represented by (*x,y*) data pairs, are offloaded through an interface program. *LabVIEW* is used for the interface with drivers [15] for the Tektronix TDS694C oscilloscope that were modified to support rapid recording to files as well as several methods of signal processing.

In addition to providing an automated means of acquiring and processing data from the oscilloscope, this method allowed for increased recording depth by simultaneously offloading the data as it was captured. The readings are then displayed in the time and frequency domains as graphed waveforms, using LabVIEW's scripting capability on a Dell Inspiron 8500. The work bench layout is shown in Fig. 5.

This output format allows for data to be filtered by locating key areas of interest in the frequency domain, making it easier to identify magnitude (*x,y*) pairs that can provide a distinct method for describing a trace signature for the various attacks. These attack traces would then be maintained in the system's signature database and can be matched by the application server to identify an attack based on the diagnostic battery readings reported by the PDA.

A. Attack Experiments

For the battery exhaustion tests, flooding and DoS attacks were used. This research also investigated other Wi-Fi and

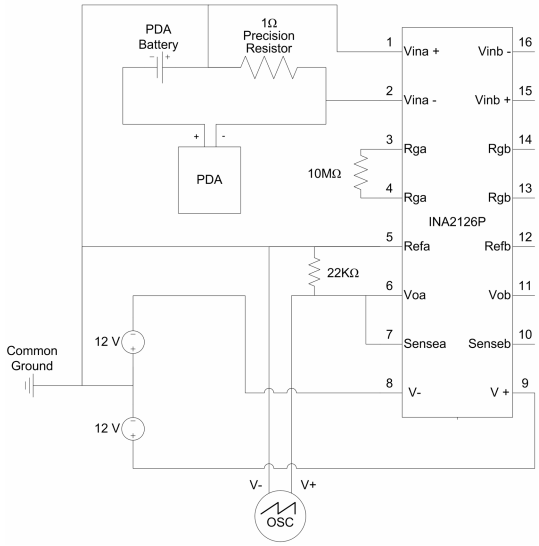


Fig. 4. Amplification circuit used in attack experiments.

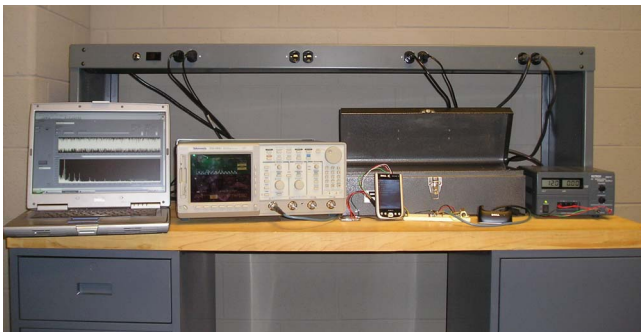


Fig. 5. Attack lab experiment setup.

Bluetooth attacks to gain an appreciation of possible attacks that could confront PDAs and smart phones shown in Table I. Libraries of attack code, such as *www.metasploit.com*, *trifinite.org*, and *www.remote-exploit.org* were examined. Additionally, *SANS.org*, the *CERT/CC* at Carnegie Mellon, and *Symantec, Inc*. provided libraries of exploit descriptions. SANS provides a "Top 20" listing of the most common attacks, which aided in selecting the short list of directed attacks used in these experiments.

The small mobile computing devices used in this research are shown in Table II. These devices suited the testing parameters because they employ smart batteries, similar OSs, Wi-Fi, and Bluetooth. The selected devices were connected to the monitoring circuit shown in Fig. 4 and baseline measurements were taken with Bluetooth and Wi-Fi radios enabled. Each system was set with the maximum brightness and its processor throttling off. These measurements were taken over the span of approximately five seconds to create a detailed characteristic of the device's typical current usage. Using a windowing function to reduce noise from the abrupt halt of the sample, the characteristic is then converted from the time domain to the frequency domain. From the frequency domain, it is then possible to compare periodic changes in the device's behavior. After extensive initial testing, it was determined that an effective setting for capturing the attacks was to sample at a rate of 10KHz with a depth of approximately five seconds after starting the attack. With a base model for each device established for Bluetooth and Wi-Fi, a series of attacks was then run and compared to the baseline in order to determine a unique and repeatable signature for that attack per each device type.

B. Experiment Results

During the course of testing a series of base readings were recorded for each of the devices. The resulting characteristic for the Axim X51v is shown in Fig. 6. The frequency domain clearly shows limited activity, except in the very low frequency range which can be ignored as noise. This shows that the base state of the device has a clearly visible and relatively quiet trait. However, when an attack such as a SYN Flood, shown in Fig. 7, or a Xmas Tree stealth scan, depicted in Fig. 8, is launched against the device a substantial amount of battery response activity can be observed. This activity, while changing in magnitude, consistently occurs in the same frequency range as depicted by the characteristic trace. By observing the attributes of the attacks in the aforementioned figures it becomes apparent that each attack has a set of unique and reoccurring characteristics that differ from the base behavior of the device. This demonstrates that a trace signature can be developed for an attack based on the device's instantaneous current usage during the event.

TABLE I.
LIST OF ATTACKS

Attack	Category	Vector	Propagation
SYN Flood	Flooding	Notebook w/ *hping2*	Wi-Fi
Stealth Scan	UDP Port Scan	Notebook w/ *nmap*	Wi-Fi
Xmas Scan	Invasive Scan	Notebook w/ *nmap*	Wi-Fi
BlueJacking	Messaging	PDA w/ Smurf tool	Bluetooth
BlueSmack	DoS	Notebook w/ adapter	Bluetooth

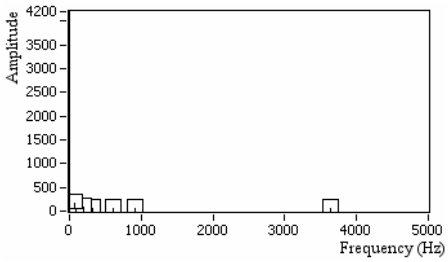
C. Analysis

Upon capturing a distinguishing attribute which is thought to represent an attack, key magnitude (*x,y*) pairs are extracted from the characteristic. Low frequency events in the 1Hz to 100Hz range are ignored as they commonly represent noise. The remaining points are selected in a greatest magnitude first order with a fixed buffer on either side to avoid inadvertent re-sampling distortions. The relative frequency location of each key pair as well as their normalized magnitudes, obtained by dividing each magnitude by the number of data pairs in a sample, can then be compared with other captured suspect characteristics. The confidence interval resulting from the comparison then determines the likelihood that the trace signature represents a given attack.

The Bluetooth base readings are shown in Fig. 9. A Bluetooth messaging and OS fingerprinting tool called *Smurf* from *http://www.gatefold.co.uk/smurf/* was used to conduct a BlueJacking exploit shown in Fig. 10 to intrude directly from PDA to another PDA. BlueSmack, depicted in Fig. 11, is a DoS attack using the *l2ping* command tool from the *Bluez* protocol stack. These low powered attacks yielded discernable results, once the *y*-scale was reduced. In the Bluetooth attacks sampled by the oscilloscope, the Wi-Fi radio was disabled. However, the Bluetooth attacks were later run against the devices with the Wi-Fi radio enabled and the PDA client with B-SIPS was able to successfully detect the attacks and report

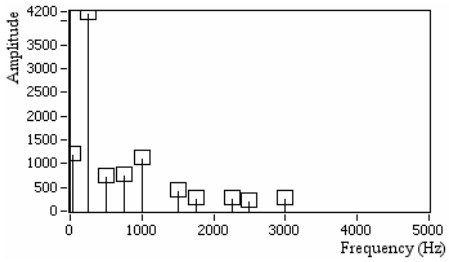
TABLE II.
PDA AND SMART PHONE CAPABILITIES

Model	Processor	OS	Battery
Dell Axim X51v	Intel XScale PXA270 624 MHz	WinMobile 5.0	Li-Ion 1100 mAh
Dell Axim X51	Intel XScale PXA270 520 MHz	WinMobile 5.0	Li-Ion 1100 mAh
Dell Axim X50v	Intel XScale PXA270 624MHz	WinMobile 2003 2nd Ed	Li-Ion 1100 mAh
Dell Axim X30	Intel XScale WMMX 624MHz	WinMobile 2003 2nd Ed	Li-Ion 1000 mAh
HP iPAQ hx2795b	Intel XScale PXA270 624MHz	WinMobile 5.0	Li-Ion 1440 mAh
HP iPAQ 4155	Intel XScale PXA255 400MHz	WinMobile 2003 2nd Ed	Li-Ion 1000 mAh
Cingular 8125	TI OMAP850 200 MHz	WinMobile 5.0 Phone	Li-Polymer 1250 mAh
Samsung i730	Intel XScale PXA272 520MHz	WinMobile 5.0 Phone	Li-Ion 1000 mAh



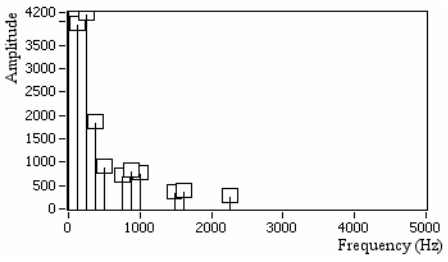
Bluetooth turned off.

Fig. 6. Wi-Fi baseline for X51v.



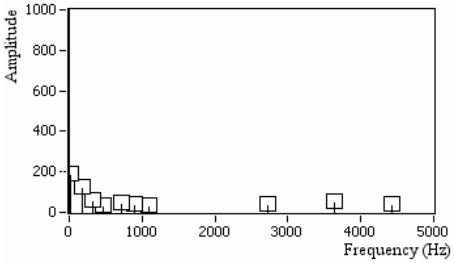
hping -S -c 10000 -i u100

Fig. 7. SYN flood against Axim X51v.



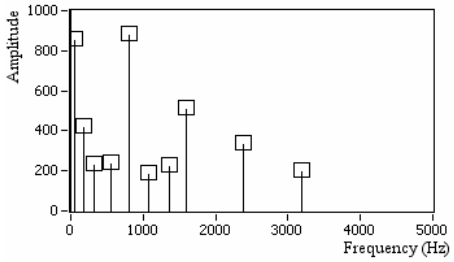
nmap -sX -O -p- -PI -PT -T5 -v

Fig. 8. Xmas tree stealth scan of X51v.



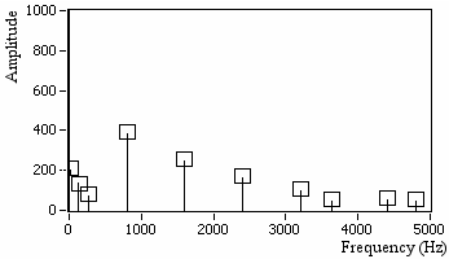
Wi-Fi turned off.

Fig. 9. Bluetooth baseline for X51v.



BlueSmurf v0.2 in "continuous" search mode

Fig. 10. BlueJacking trace of X51v.



l2ping -s 600 -c 10000

Fig. 11. BlueSmack DoS against X51v.

to the server. Lastly, this research is characterizing the device battery drain to optimize the B-SIPS client coding. The assessment of 10 trials of 10 Axim X51 PDAs is shown in Fig. 12. The research goal is to minimize battery power use while maximizing the device's ability to detect Bluetooth and Wi-Fi propagated attacks and illicit activities with B-SIPS.

V. Conclusion and Future Work

The concept of employing battery constraints as a means of intrusion detection is a relatively new capability that was only recently made possible by developments in smart battery and ACPI technologies. The B-SIPS design offers a hybrid intrusion detection method that can serve to protect small mobile computers from anomalous activity which seeks to drain battery power excessively. This research asserts that small mobile hosts in a net-centric environment can be protected by B-SIPS, which triggers alerts based on power utilization threshold breaches detected by an innovative instantaneous current-based threshold algorithm. The next step of B-SIPS research will investigate and develop trace signatures for Bluetooth and some existing wireless network-based attacks for matching in the signature base.

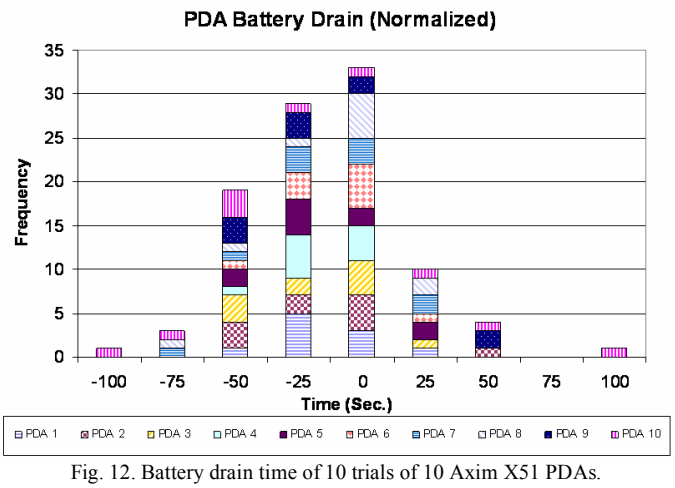


Fig. 12. Battery drain time of 10 trials of 10 Axim X51 PDAs.

References

[1] T. K. Buennemeyer, F. Munshi, et al., "Battery-sensing intrusion protection for wireless handheld computers using a dynamic threshold calculation algorithm for attack detection," in *the 40th Annual Hawaii International Conference on System Sciences (HICSS-40)* Waikoloa, Hawaii, 2007.

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

[3] ACPI, "Advanced configuration and power interface," http://www.acpi.info, 2005.

[4] SBS_Forum, "Smart battery system implementers forum," http://www.sbs-forum.org, 2005.

[5] SMBus, "System management bus," http://www.smbus.org, 2005.

[6] E. Thompson, "Smart batteries to the rescue," http://www.mcc-us.com/SBSRescue.pdf, 2000.

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

[8] T. Martin, M. Hsiao, et al., "Denial-of-service attacks on battery-powered mobile computers," in *Second IEEE Annual Conference on Pervasive Computing and Communications.* , Orlando, FL, 2004.

[9] M. Brownfield, G. Yatharth, et al., "Wireless sensor network denial of sleep attack," in *the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop. West Point, NY*, 2005.

[10] R. Racic, D. Ma, et al., "Exploiting MMS vulnerabilities to stealthily exhaust mobile phone's battery," in *the 15th Annual USENIX Security Symposium* Vancouver, BC, 2006.

[11] T. K. Buennemeyer, G. A. Jacoby, et al., "Battery-sensing intrusion protection system," in *the Seventh Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop*, West Point, NY, 2006.

[12] MSDN, "Microsoft .NET framework developer center," http://msdn.microsoft.com/netframework/, 2006.

[13] J. Polastre, J. Hill, et al., "Versatile low power media access for wireless sensor networks," in *ACM International Conference on Embedded Networked Sensor Systems (Sensys)*, 2004.

[14] G. A. Jacoby and N. J. Davis, "Battery-based intrusion detection," in *the IEEE Global Telecommunications Conference (GLOBECOM '04). Dallas, TX*, 2004.

[15] National_Instruments, "LabVIEW certified plug and play driver," http://sine.ni.com/apps/, 2006.