Denial-of-Service Attacks on Battery-powered Mobile Computers

Thomas Martin, Michael Hsiao, Dong Ha, Jayan Krishnaswami

Presented by Kevin Kardian

CS 525M Mobile Computing

Outline

- Introduction
- Background
- Motivation
- Power Attack Experiments
- Potential Improvements
- Conclusions

Introduction

- **Sleep deprivation attack:**
  - **A denial of service attack on a battery operated device**
  - **Designed to completely drain a battery**
  - **Allows attacker to move on after battery is drained**
- **Three distinct methods for draining a battery:**
  - **Service request power attacks**
  - **Benign power attacks**
  - **Malignant power attacks**

Introduction (cont.)

- Increasing use of wireless devices
  - Society relies more heavily on these devices
  - Need for security increases as these devices become targets
- Sleep deprivation attacks have a potentially massive impact
  - Batteries with an expected life of a month drained within a day

Outline

- Introduction
- Background
- Motivation
- Power Attack Experiments
- Potential Improvements
- Conclusions

Background

- Sleep deprivation on wireless sensor networks
  - First mention of attacks designed to drain batteries of mobile devices
  - General purpose devices are equally, if not more vulnerable
- Power analysis of encryption devices
  - Has been shown to reveal large portions of encryption keys
  - Represents an attack on security rather than functionality

Background (cont.)

- **Authentication in distributed environments**
  - **Design expected to share characteristics primarily with X.509**
  - **Depends on certificates from a remote authority**
  - **That authority does not need to maintain contact**
- **Low power software design**
  - **Useful for detecting attacks and reducing the power in associated services**
- **Peak power estimation**
  - **Primarily employed to generate the attacks used in experiments**

Outline

- Introduction
- Background
- Motivation
- Power Attack Experiments
- Potential Improvements
- Conclusions

Motivation

What makes an attack effective?

- **Maximize power consumption**
  - **Target subsystems that will have the most effect**
  - **Greatest difference between active and idle power**
  - **Longest time spend in active mode**
- **Present the illusion that the system is behaving normally**
  - **User may think that the battery is defective**

Motivation

How effective can an attack get?

- **Normal usage patterns have devices in an idle state for a vast majority of the time**
- **The battery life can be reduced by a factor equal to P_{active}/P_{idle}**
- **Examples of this ratio:**
  - **Commercial PDAs = 280**
  - **Experimental PDAs = 30**
  - **Notebook computers = 2 to 4**

Outline

- Introduction
- Background
- Motivation
- Power Attack Experiments
- Potential Improvements
- Conclusions

Experiments

General Methodology

- **3 Platforms:**
  - **IBM Thinkpad T23 notebook**
  - **Compaq iPAQ 3760 PDA**
  - **Compaq Itsy PDA**
- **Agilent 3458A digital multimeter**
  - **Set to a sampling rate of 10,000 samples/second**
  - **Averaged over 100 samples**
  - **Synchronized to activate on external trigger**

Experiments

General Methodology (cont.)

- **Service request attack**
  - **Repeated SSH requests**
  - **Correct username, incorrect password**
- **Benign power attack**
  - **Animated GIF that displays the same frame repeatedly**
  - **Compared against a non-animated version**
- **Malignant power attack**
  - **Program that performed I/O on an array**
  - **Variable array size**

Experiments

Service Request Attack

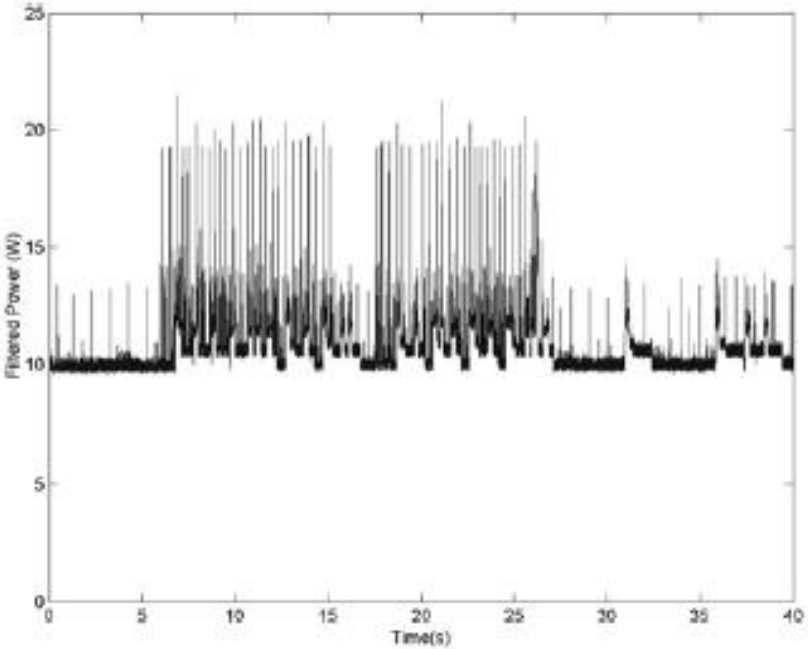

Figure 1. Requests made to SSH server on the Thinkpad with wrong password.

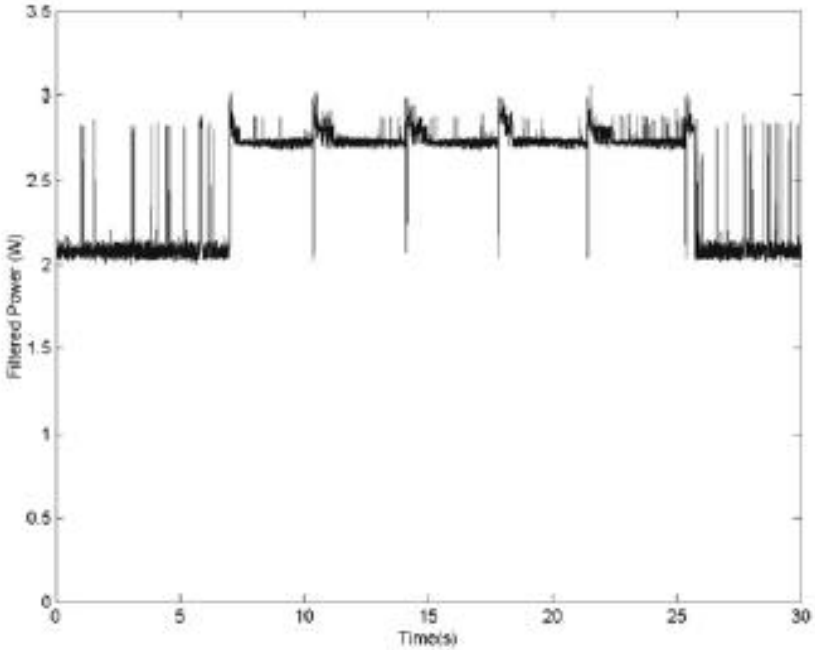

Figure 2. Requests made to SSH server on the iPAQ with wrong password.

Experiments

Benign Power Attack

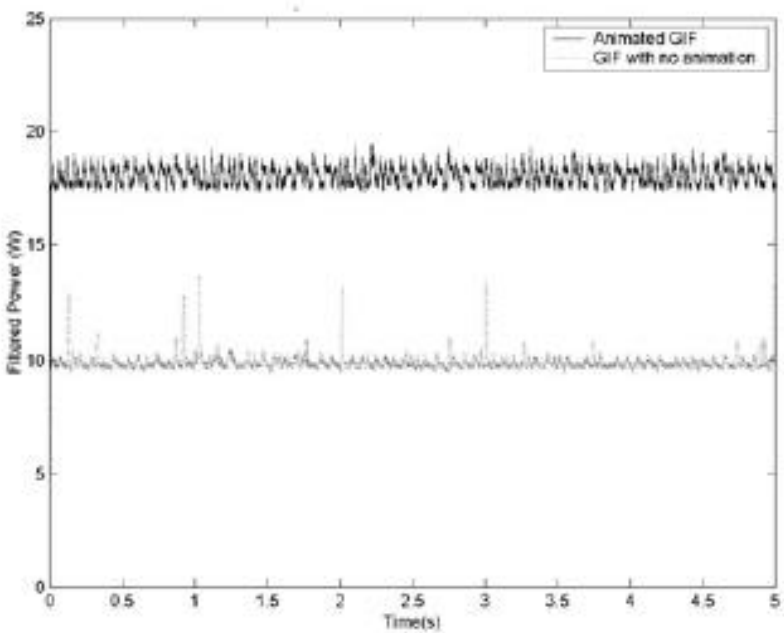

Figure 3. Comparison of power consumption of animated GIF and non-animated GIF on the Thinkpad

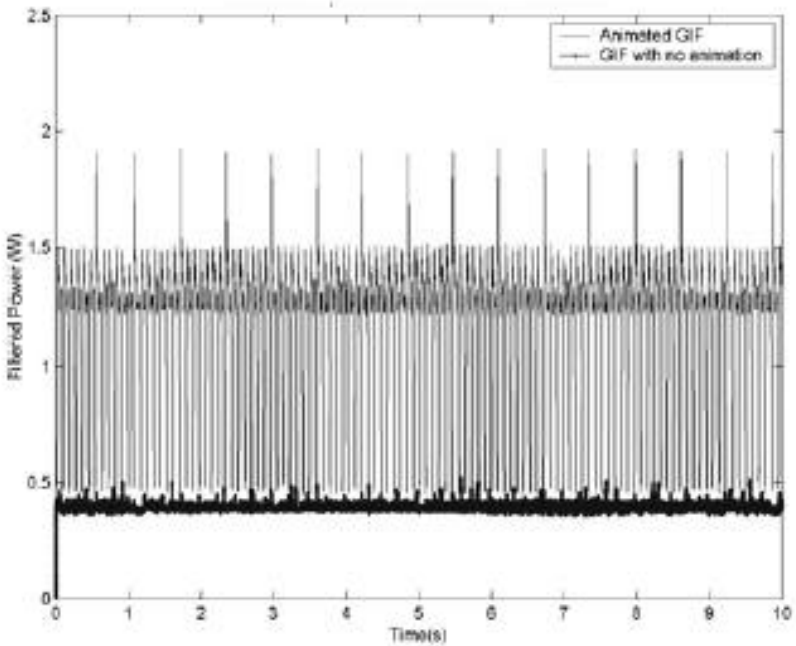

Figure 4. Comparison of power consumption of animated GIF and non-animated GIF on iPAQ

Experiments

Malignant Power Attack

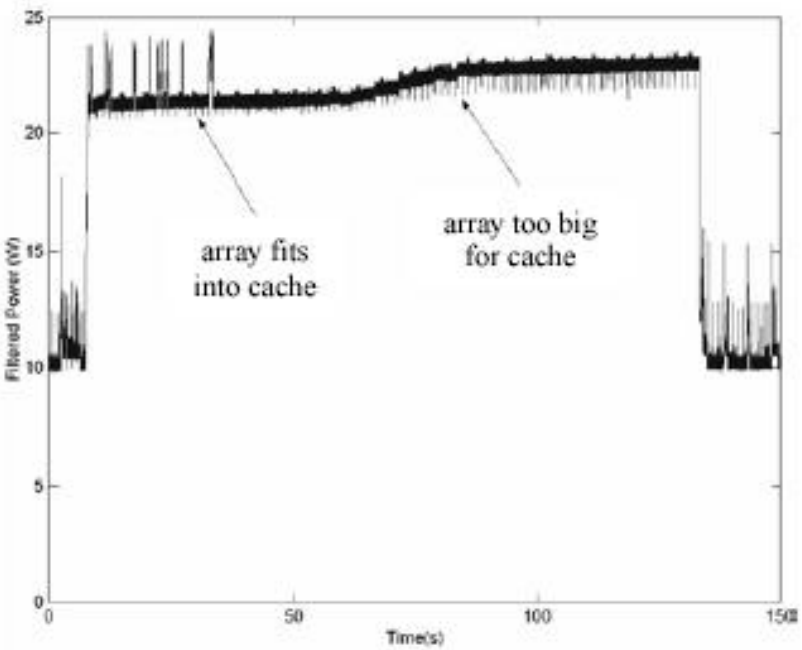

Figure 5. Power consumption during malignant power attack on the Thinkpad

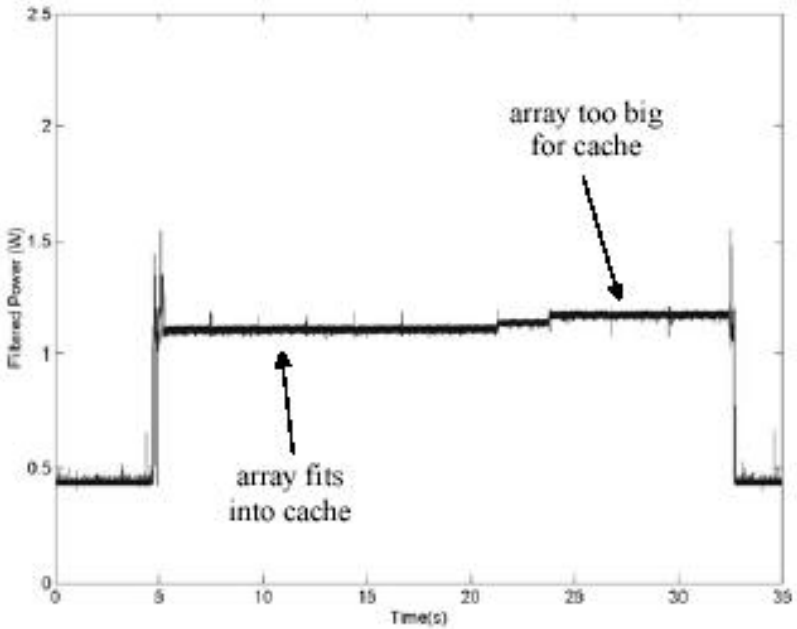

Figure 6. Power consumption during malignant power attack on the iPAQ

Experiments

Malignant Power Attack (cont.)

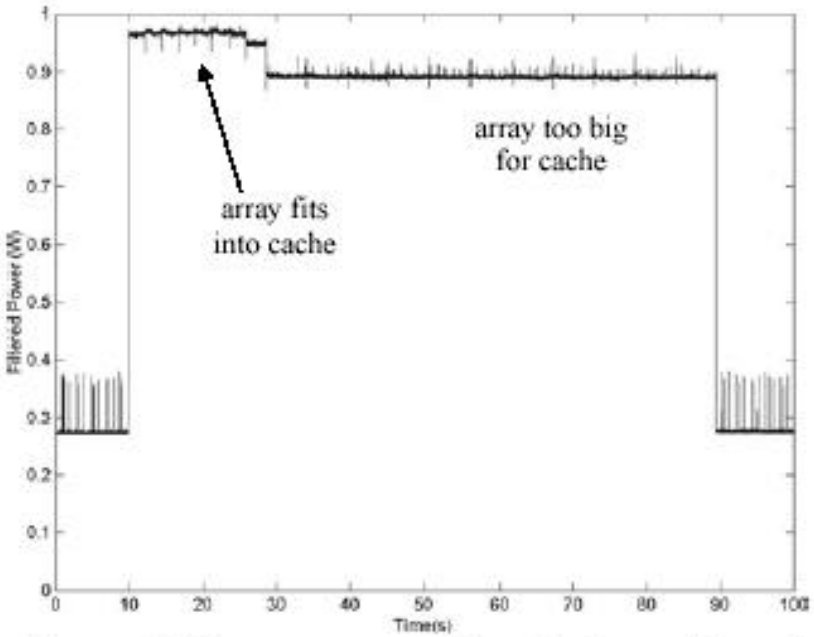

Figure 7. Power consumption during malignant power attack on the Itsy at 206 MHz

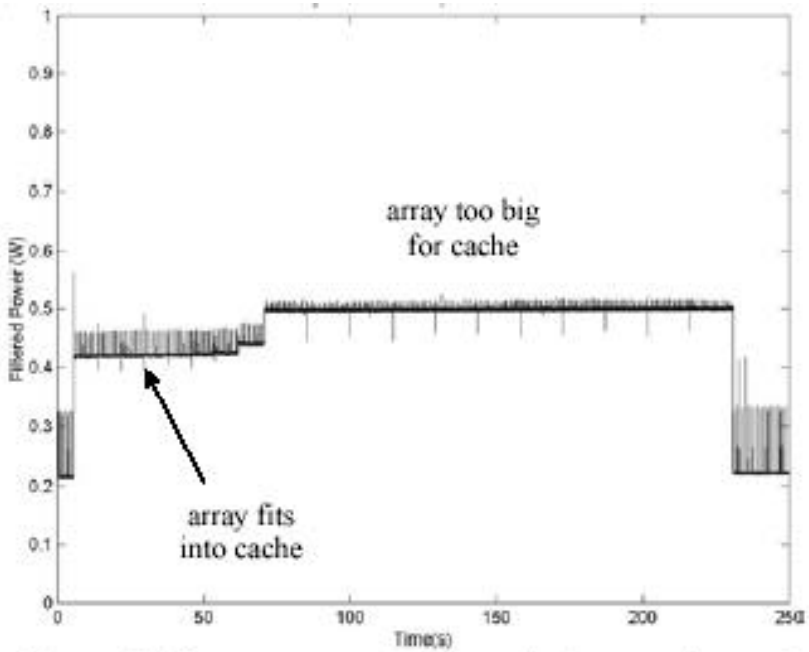

Figure 8. Power consumption during malignant power attack on the Itsy at 59 MHz

Outline

- Introduction
- Background
- Motivation
- Power Attack Experiments
- Potential Improvements
- Conclusions

Potential Improvements

Multi-layer Authentication

- **Energy consumption of a service is not constant**
- **Preventing an unauthorized service request from fully executing should save power**
- **After a predetermined amount of time (T), each service request should be authenticated**

Potential Improvements

Multi-layer Authentication (cont.)

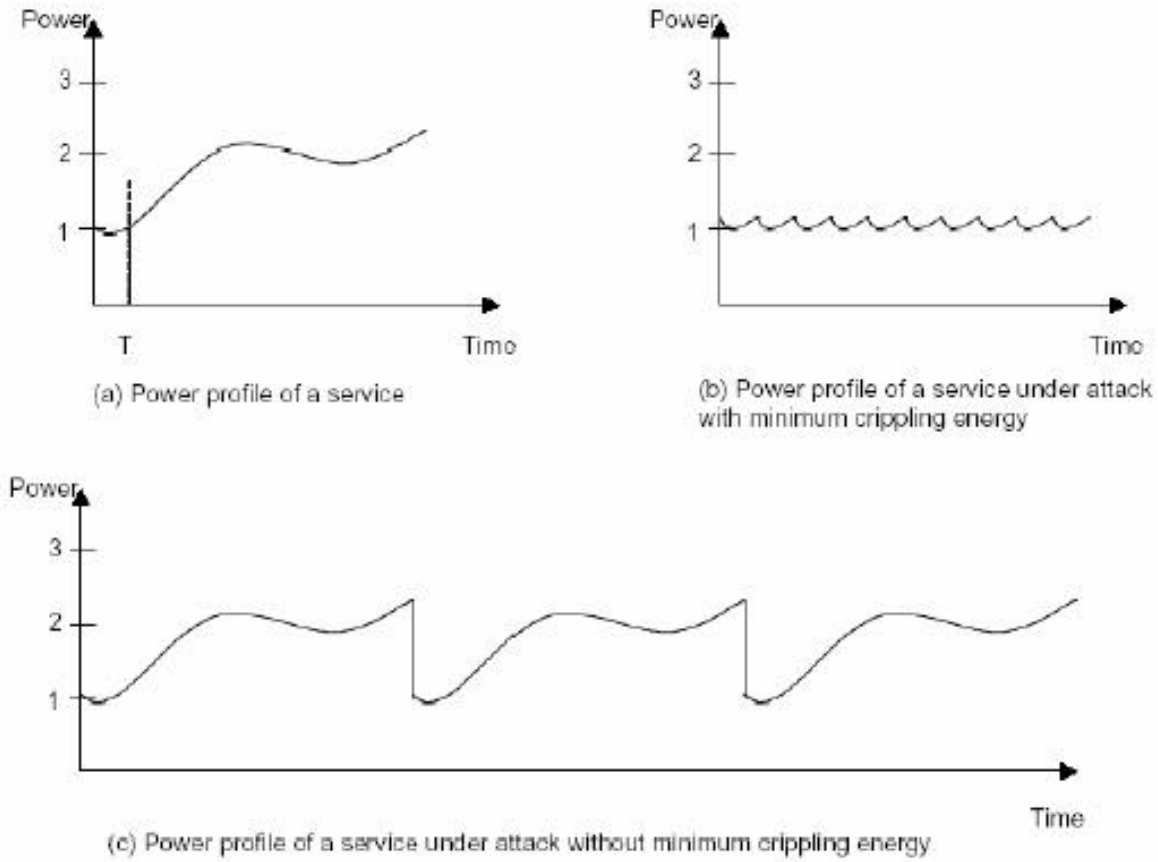

Figure 9. Power profiles of a service showing the concept of the crippling energy level

Potential Improvements

Crippling Energy Level

- **Defined as the amount of energy required to fully drain a battery in a given amount of time**
- **Crippling Energy Level <= E X T / L**
  - **E = total energy available**
  - **L = desired battery lifetime**
- **Several layers can be used**
  - **Each layer represents a more powerful authentication**
  - **Maintains low power overhead while keeping authentication difficult to defeat**

Potential Improvements

Energy Signature Monitoring

- **Validate dynamic energy signatures against known energy signatures**
- **Handling known signatures could prove difficult**
  - **Cannot generate a signature for every possible program execution**
  - **Memory constraints limit the total number of signatures stored**
- **Should be supplemented with some other form of intrusion detection**
  - **Example: Only compare signatures when the desired lifetime of the battery can not be assured.**
  - **Energy overhead could otherwise prove counter-productive**

Outline

- Introduction
- Background
- Motivation
- Power Attack Experiments
- Potential Improvements
- Conclusions

Conclusions

- Each service has different effects on power consumption
- Cache performance differs between potential victims
- Power-secure architecture is capable of guaranteeing a minimum battery life