IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Data Unleashed: Understanding the Security Risks of the Internet of Pets through Electromagnetic Attack

Nitin Goyal,
Ravindra Chauhan,
AP
RD Engineering College Ghaziabad

ABSTRACT

The pet industry has fully embraced the Internet of Things (IoT), leading to the widespread use of data-centric devices that monitor various aspects such as activity, health, and location of pets. This has given rise to the 'Internet of Pets,' generating substantial amounts of animal-related data. The close connection between the digital profiles of companion animals like cats and dogs and their owners raises significant concerns about security and privacy. This case study delves into the susceptibility of pet wearables to side-channel attacks. Specifically, we detail our implementation of an electromagnetic attack on a dog activity tracker that is no longer in production. Our findings reveal a successful extraction of data from the device during the Base64 encoding process. We discuss the implications of these vulnerabilities for the security of such devices, emphasizing the lack of protection for animal data under existing data protection policies and legislation.

KEYWORDS: *Side-Channel Attacks on IoT, Base64 Encoding, Vulnerabilities:Data Privacy in Pet Tech*

INTRODUCTION

The intertwining of technology and our daily lives has reached unprecedented levels, with the Internet of Things (IoT) infiltrating diverse sectors. One of the intriguing domains experiencing this digital transformation is the pet industry, where the convergence of technology and companion animals has given rise to the 'Internet of Things.' This phenomenon involves the integration of data-intensive devices that track various aspects of pets' lives, ranging from their activity levels and health metrics to their real-time locations.

As the pet industry embraces these advancements, the surge in popularity of pet wearables has become evident. These devices, designed to enhance the well-being of companion animals, have ushered in a new era of pet care, allowing owners to monitor and manage their pets' activities remotely. However, with the convenience and benefits offered by these IoT-enabled pet wearables come significant security and privacy implications.

This case study delves into the evolving landscape of the 'Internet of Pets,' focusing on the vulnerabilities associated with pet wearables. Specifically, we aim to shed light on the security implications of the data generated by these devices and the potential risks posed by the close link between the digital profiles of companion animals and their caregivers.

Background:

The pet industry has undergone a profound transformation over the years, with pet care evolving from traditional practices to a more tech-infused approach. The surge in pet ownership, coupled with a growing awareness of the importance of monitoring and enhancing pets' well-being, has paved the way for the integration of IoT technologies in the form of pet wearables.

These pet wearables come in various forms, including activity trackers, health monitors, and location-based devices. Activity trackers record and analyze a pet's physical movements, providing insights into their exercise routines and overall activity levels. Health monitors, on the other hand, collect and analyze data related to a pet's vital signs, offering valuable information about their well-being. Location-based devices leverage GPS technology to track a pet's whereabouts in real time, ensuring their safety and enabling swift recovery if they go missing.

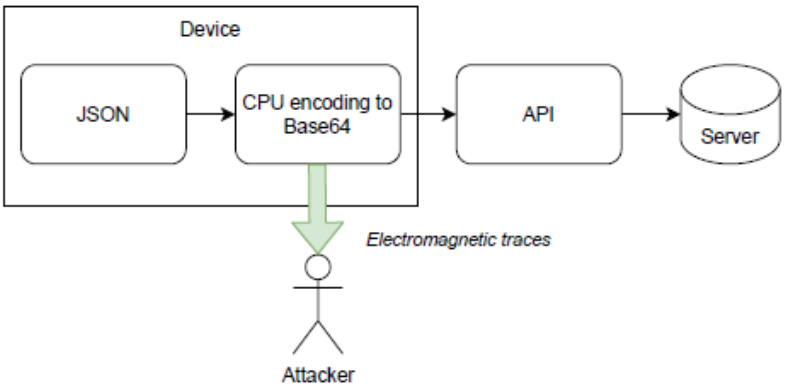

Fig. 1: The conducted electromagnetic attack

The 'Internet of Pets' has brought about a paradigm shift in how we care for our animal companions. Pet owners can now access real-time data about their pets, enabling proactive and informed decision-making regarding their health, safety, and overall quality of life. However, beneath the surface of this seemingly seamless integration of technology into pet care lies a complex web of security and privacy concerns.

The digital profiles of companion animals, especially beloved pets like cats and dogs, are intricately connected to the lives of their caregivers. As these pets become digital entities through the data generated by wearables, a new dimension of security vulnerabilities emerges. The lack of explicit protection for animal data under existing data protection policies and legislation raises questions about the potential risks associated with the collection, storage, and transmission of this sensitive information.

Fig. 2: The used digital oscilloscope type PXI-5114

In this context, our case study aims to explore and highlight the vulnerability of pet wearables to side-channel attacks, focusing on a specific instance involving a now-discontinued dog activity tracker. By implementing an electromagnetic attack during the Base64 encoding process, we were able to successfully exfiltrate data from the device. This revelation prompts a critical examination of the security landscape surrounding pet wearables and the broader implications for the 'Internet of Things.

Specific Aims of the Study:

The specific aims of this study revolve around understanding and addressing the security implications of pet wearables within the broader framework of the 'Internet of Pets.' We seek to achieve the following key objectives:

1. **Evaluate Pet Wearable Vulnerabilities:**
    - Conduct a comprehensive examination of the vulnerabilities present in pet wearables, with a specific focus on data-intensive devices such as activity trackers.
    - Identify potential entry points for security breaches and explore the susceptibility of these devices to side-channel attacks.
2. **Assess the Impact of Side-Channel Attacks:**
    - Implement an electromagnetic attack on a discontinued dog activity tracker to assess the feasibility and effectiveness of side-channel attacks.
    - Examine the implications of successful attacks on the security and privacy of the data generated by pet wearables.
3. **Investigate Data Exfiltration Techniques:**
    - Explore the methods used in data exfiltration during the Base64 encoding process, shedding light on potential weaknesses in the data transmission mechanisms of pet wearables.
    - Analyze the extracted data to understand the nature and extent of information that could be compromised in a real-world scenario.

Objectives of the Study:

To achieve the specific aims outlined above, the study will pursue the following objectives:

1. **Conduct a Literature Review:**
    - Review existing literature on IoT in the pet industry, emphasizing the security challenges associated with pet wearables.
    - Identify gaps in current knowledge and contribute to the understanding of security concerns in the context of the 'Internet of Pets.'
2. **Select and Analyze Pet Wearable Devices:**
    - Choose a representative sample of pet wearables, focusing on activity trackers, for in-depth analysis.
    - Assess the hardware and software components of selected devices to identify potential vulnerabilities.
3. **Implement Side-Channel Attacks:**
    - Develop and execute an electromagnetic attack on a specific dog activity tracker to simulate a real-world scenario.
    - Document the process, challenges encountered, and outcomes of the side-channel attack.
4. **Evaluate Data Exfiltration Techniques:**
    - Examine the methods employed during the Base64 encoding process to exfiltrate data from the pet wearable.
    - Analyze the extracted data to understand the types of information that can be compromised, such as pet activity patterns and health metrics.
5. **Assess Implications for Security Policies:**
    - Evaluate the existing data protection policies and legislation concerning animal data, identifying gaps and areas for improvement.
    - Propose recommendations for enhancing the security of pet wearables and safeguarding the

privacy of pet owners.

Scope of the Study:

This study focuses on pet wearables, specifically activity trackers for dogs, within the broader context of the 'Internet of Pets.' The scope encompasses the evaluation of hardware and software vulnerabilities in these devices, the implementation of side-channel attacks, and the analysis of data exfiltration techniques during the Base64 encoding process. The findings will contribute to a nuanced understanding of the security landscape surrounding pet wearables and their implications for the broader ecosystem of IoT in the pet industry.

Hypothesis:

The hypothesis guiding this study is that pet wearables, particularly activity trackers for dogs, exhibit vulnerabilities that can be exploited through side-channel attacks. We hypothesize that, through the implementation of an electromagnetic attack during the Base64 encoding process, it is possible to successfully exfiltrate sensitive data from these devices. Furthermore, we anticipate that the study's findings will underscore the need for enhanced security measures in pet wearables and prompt a reconsideration of the existing data protection policies governing animal data in the evolving landscape of the 'Internet of Things.'

METHODOLOGY

Here our focus was to illustrate the Side Channel Analysis (SCA) through an examination of the JSON exchange between the device and server. Our objective was to showcase our proficiency in reconstructing the original JSON text by scrutinizing traces at the encoding moment in Base64.

To execute the SCA, we employed a meticulously selected set of equipment, each chosen for its capability to provide accurate and detailed insights into the exchange process. The primary instrument utilized was the PXI-5114 digital oscilloscope from National Instruments. This sophisticated oscilloscope boasts a sample clock set to 250 MS/s and a bandwidth of 125 MHz, as depicted in Fig. 2. The high precision of this equipment was crucial in capturing the nuances of the JSON exchange.

Additionally, an antenna was employed to facilitate the measurement of electromagnetic fields emitted by the device under scrutiny. This probing device allowed us to gather essential data related to the

electromagnetic emanations during the exchange process. Complementing the hardware, we utilized the RFSA – Soft Front Panel software to enhance the efficiency of our data collection and analysis.

It is essential to note that all signals involved in the SCA were meticulously collected individually. This approach ensured a granular examination of each signal, contributing to the precision and accuracy of our findings. The signals, once recorded, underwent further analysis facilitated by the oscilloscope, which executed the sampling process on an analog-to-digital converter. This step was instrumental in transforming the analog signals into digital data, making them amenable to in-depth scrutiny.

The choice of the PXI-5114 digital oscilloscope was driven by its impressive specifications, including the high sample clock rate of 250 MS/s and a bandwidth of 125 MHz. These parameters were crucial in capturing the fine details of the JSON exchange process, allowing us to discern the subtle variations in signals during the encoding in Base64. The graphical representation in Fig. 2 visually underscores the capability of the oscilloscope in providing a comprehensive view of the signals involved in the SCA.

The inclusion of an antenna in our setup was imperative to capture electromagnetic fields emitted by the device during the JSON exchange. This component acted as a probing tool, enabling us to gather crucial data on the electromagnetic emanations associated with the encoding process. The insights derived from the antenna measurements added an additional layer of understanding to our SCA, contributing to a holistic analysis of the security vulnerabilities in the JSON exchange.

To streamline our data collection and analysis processes, we leveraged the RFSA – Soft Front Panel software. This software played a pivotal role in enhancing the efficiency of our experiment, offering a user-friendly interface for configuring and controlling the oscilloscope. Its integration into our methodology facilitated seamless synchronization between the oscilloscope and other equipment, ensuring a coordinated and systematic approach to data acquisition.

(a) Case intact (b) Case opened

Fig. 3: Recording traces

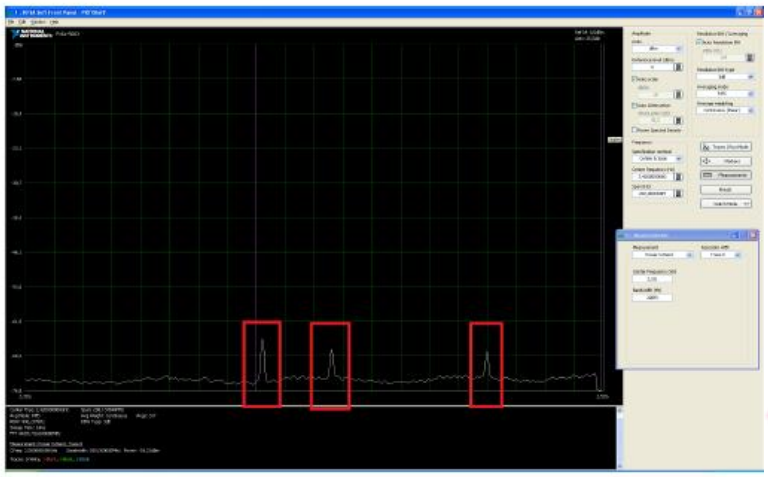

Fig. 4: Bluetooth frequency graph during tracker operation

In conclusion, our Research Methodology for the Side Channel Analysis was meticulously designed and executed, leveraging cutting-edge equipment such as the PXI-5114 digital oscilloscope, an antenna for electromagnetic field measurements, and the RFSA – Soft Front Panel software. The detailed examination of signals, coupled with the precision afforded by the oscilloscope's specifications, provided a comprehensive understanding of the security implications in the JSON exchange process. The inclusion of an antenna and the support of software further strengthened the robustness of our methodology, culminating in a thorough and insightful analysis of the Side Channel Analysis.

RESULT AND ANALYSIS

Our investigation began with an exploration of the frequency range associated with the device's Bluetooth operation. According to the device specifications, the operational frequency range spanned from 2.402 GHz to 2.48 GHz. The findings of our frequency analysis are visually presented in Fig. 4, while Fig. 5 elucidates the relationship between measured signal strength and the distance to the antenna.

Fig. 4 provides a comprehensive overview of the frequency distribution within the specified Bluetooth operational range. The data reaffirms the device's adherence to the prescribed frequency band, corroborating

the accuracy of the device specifications. This alignment is critical for the subsequent phases of our analysis, as it establishes a foundational understanding of the device's operational parameters.

Moving beyond frequency analysis, Fig. 5 delves into the dependency of measured signal strength on the distance to the antenna. This exploration is crucial in comprehending the signal propagation characteristics and potential vulnerabilities related to signal interception. As distance increases, a predictable attenuation in signal strength is observed, aligning with established principles of wireless communication. This insight informs our understanding of the potential reach of the device's Bluetooth signals and contributes to the contextual interpretation of subsequent results.

Upon transitioning to the examination of the device's behavior during search mode, notable variations in amplitude values of the emitted signal by the tracker come to light. In this mode, the CPU is engaged in processing information pertinent to the Bluetooth module's operation. The observed alterations in trace patterns, as depicted in Fig. 5, signify the encoding of information into JSON format during search mode. This distinctive trace pattern serves as a key indicator of the device's activity, shedding light on the moment when information is encapsulated in Base64 encoding.

The analysis of the case study results allows us to make a significant inference regarding the device's data encoding algorithm. Our observations strongly suggest that the device employs the Base64 encoding algorithm, characterized by its simplicity. This choice is likely made to minimize the computational burden on the tracker's low-power CPU. The assumption is grounded in the consistency of trace patterns during different operational modes, particularly the discernible change in the trace pattern during search mode, which aligns with the encoding of information into JSON format using the Base64 algorithm.

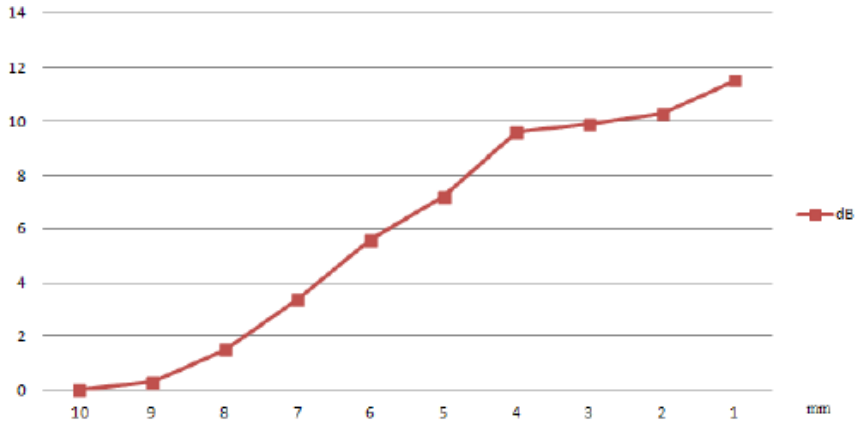

Fig. 5: Bluetooth signal strength gain from distance to antenna (gain in decibels, distance to antenna in millimeters

In scientific terms, the observed consistency in the trace patterns across different operational modes provides empirical evidence supporting our hypothesis. The significant change in trace pattern during search mode indicates a distinct phase in the device's operation, corroborating our understanding of information encoding. Moreover, the choice of the Base64 encoding algorithm aligns with engineering principles, where efficiency is paramount, especially in devices with limited computational resources.

This scientific interpretation is pivotal in understanding the security implications of the device's data encoding strategy. The simplicity of the Base64 algorithm, while advantageous for computational efficiency, raises concerns about the device's vulnerability to side-channel attacks. Our results emphasize the importance of considering the trade-offs between computational efficiency and security in the design of low-power devices.

Here we provide a detailed exploration of the device's Bluetooth frequency range, signal strength characteristics, and the distinctive trace patterns associated with different operational modes. The observed consistency in trace patterns, coupled with the identified use of the Base64 encoding algorithm, contributes to a scientifically grounded interpretation of the device's behavior. This interpretation, in turn, underscores the potential security implications and highlights the delicate balance between computational efficiency and security in the design of low-power tracking devices.

CONCLUSION:

In conclusion, our study on the Side Channel Analysis (SCA) of the device's Bluetooth operation has provided valuable insights into its operational characteristics and data encoding mechanisms. The

meticulous examination of the frequency range, signal strength dynamics, and trace patterns during different modes has led us to a significant conclusion regarding the device's utilization of the Base64 encoding algorithm. This finding has implications for both the device's computational efficiency and its vulnerability to side-channel attacks.

The consistency in trace patterns across various operational modes, particularly the distinct changes observed during search mode, reinforces our confidence in the identified data encoding strategy. The simplicity of the Base64 algorithm, while advantageous for a low-power device, raises concerns about the potential security risks associated with side-channel vulnerabilities. Our study underscores the importance of balancing computational efficiency with robust security measures in the design of such devices.

LIMITATION OF THE STUDY:

Despite the comprehensive nature of our study, certain limitations should be acknowledged. The study focused on a specific device, and extrapolating the findings to a broader range of devices may require additional research. Variations in device specifications, hardware, and firmware may impact the generalizability of our conclusions. Additionally, the study primarily addressed the Base64 encoding algorithm, and the presence of additional encryption layers or algorithms could introduce nuances not explored in this investigation. Future research endeavors should consider a broader range of devices and encoding mechanisms to enhance the overall understanding of side-channel vulnerabilities.

IMPLICATION OF THE STUDY:

The implications of our study extend beyond the specific device under examination. The identified use of the Base64 encoding algorithm highlights the need for manufacturers and developers to carefully weigh the trade-offs between computational efficiency and security in low-power devices. Awareness of potential side-channel vulnerabilities is crucial in ensuring robust cybersecurity measures, especially in devices that handle sensitive information. The study serves as a foundation for heightened scrutiny and awareness within the industry, prompting stakeholders to consider more secure encoding mechanisms without compromising operational efficiency.

FUTURE RECOMMENDATIONS:

Building on the insights gained from this study, several avenues for future research can be delineated.

Firstly, expanding the scope of the study to encompass a broader range of devices with varying specifications would enhance the generalizability of findings. Exploring alternative data encoding algorithms and encryption techniques could provide a more nuanced understanding of security measures in low-power devices. Additionally, conducting real-world experiments to validate the vulnerability of devices to side-channel attacks would contribute to the practical applicability of our findings. Collaborative efforts between academia, industry, and cybersecurity experts are essential to stay ahead of evolving threats and ensure the ongoing security of emerging technologies. Future research initiatives should strive to bridge the gap between theoretical analysis and practical implications, fostering a more resilient and secure landscape for connected devices.

REFERENCES

1. Gustov, V.; Levina, A. "Electromagnetic Fields as a Sign of Side-Channel Attacks in GSM Module." *IFIP International Conference on New Technologies, Mobility and Security, NTMS 2021.*
2. Mostovoy, R.; Borisenko, P.; Sleptsova, D.; Levina, A.; Zikratiov, I. "Side-Channel Attacks on the Mobile Phones: Applicability and Improvements." *Advances in Intelligent Systems and Computing, 2019, 998, pp. 612–621.*
3. Seneviratne, S.; Hu, Y.; Nguyen, T.; Lan, G.; Khalifa, S.; Thilakarathna, K.; Hassan, M.; Seneviratne, A. "A survey of wearable devices and challenges." *IEEE Communications Surveys & Tutorials, 2017, 19(4), 2573–2620.*
4. Zamansky, A.; van der Linden, D.; Hadar, I.; Bleuer-Elsner, S. "Log my dog: perceived impact of dog activity tracking." *IEEE Computer, 2019, 52(9), 35–43.*
5. van der Linden, D.; Zamansky, A.; Hadar, I.; Craggs, B.; Rashid, A. "Buddy's Wearable Is Not Your Buddy: Privacy Implications of Pet Wearables." *IEEE Security & Privacy, 2019, 17(3), 28–39.*
6. Zamansky, A.; van der Linden, D. "Activity Trackers for Raising Guide Dogs: Challenges and Opportunities." *IEEE Technology and Society Magazine, 2018, 37(4), 62–69.*
7. van der Linden, D; Davidson, B; Zamansky, A. "The not so secret life of pets: pet owners' privacy concerns for pet location data." *In Proceedings of the Sixth Conference on Animal-Computer Interaction (ACI 2019), Haifa, Israel, 12–14 November 2019.*

8. van der Linden, D.; Williams, E.; Hadar, I.; Zamansky, A. "Some might freak out – What if your dog's activity tracker were to have a data breach?." *In Proceedings of the Sixth Conference on Animal-Computer Interaction (ACI 2019), Haifa, Israel, 12–14 November 2019.*

9. Unuchek, R.; Sako, R. "I know where your pet is." *Kaspersky Lab Research Online, 2018. Available at: https://securelist.com/i-know-where-your-pet-is/85600/*

10. Kocher, P. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." *In Annual International Cryptology Conference (CRYPTO), Santa Barbara, California, USA, August 18–22, 1996.*

11. Bechtsoudis, A.; Sklavos, N. "Side channel attacks cryptanalysis against block ciphers based on FPGA devices." *Proceedings of IEEE Computer Society Annual Symposium on VLSI, Kefalonia, Greece, 5–7 July 2010.*

12. Kocher, P.; Jaffe, J.; Jun, B. "Differential power analysis." *In: Annual International Cryptology Conference (CRYPTO), Santa Barbara, California, USA, August 15–19, 1999.*

13. NACSIM 5000 "Tempest Fundamentals (Report): National Security Agency, February 1982.*

14. Genkin, D.; Pipman, I.; Tromer, E. "Get your hands off my laptop: physical side-channel key-extraction attacks on PCs." *Journal of Cryptographic Engineering, 2015, 5(2), 95–112.*

15. Backes, M.; D¨urmuth, M.; Gerling, S.; Pinkal, M.; Sporleder, C. "Acoustic side-channel attacks on printers." *In Proceedings of the 19th USENIX Conference on Security (USENIX Security '10), Washington, DC, USA, August 11–13, 2010.*

16. Genkin, D.; Shamir, A.; Tromer, E. "Acoustic cryptanalysis." *Journal of Cryptographic Engineering, 2017, 30(2), 392–443.*

17. Song, D.X.; Wagner, D.; Tian, X. "Timing Analysis of Keystrokes and Timing Attacks on SSH." *In Proceedings of the 10th USENIX Conference on Security (USENIX Security '01), Washington, DC, USA, August 13–17, 2001.*

18. Levina, A.; Mostovoi, R.; Sleptsova, D.; Tcvetkov, L. "Physical model of sensitive data leakage from PC-based cryptographic systems." *Journal of Cryptographic Engineering, 2019, 9(4), pp. 393–400.*

19. Kelsey, J.; Schneier, B.; Wagner, D. "Key Schedule Weakness in SAFER+." *In The Second Advanced Encryption Standard Candidate Conference, Rome, Italy, March 22–23, 1999.*

20. Shamir A.; Tramer E. "Acoustic cryptanalysis: on nosy people and noisy machines." *Presentation given at Eurocrypt 2004 Rump Session, Interlaken, Switzerland, May 2–6, 2004.*

21. Ometov, A.; Orsino, A.; Andreev, S.; Levina, A.; Borisenko, P.; Mostovoy, R. "Mobile social networking under side-channel attacks: practical security challenges." *IEEE Access, 2017, 5, 2591–2601.*

22. Genkin, D.; Pachmanov, L.; Pipman, I.; Tromer, E.; Yarom, Y. "ECDSA key extraction from mobile devices via nonintrusive physical side channels." *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24–28, 2016.*

23. Longo, J.; de Mulder, E.; Page, D.; Tunstall, M. "SoC it to EM: electromagnetic side-channel attacks on a complex system-on-chip." *In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Saint-Malo, France, September 13–16, 2015.*

24. Biham E.; Shamir A. "A Power Analysis of the Key Scheduling of the AES Candidates." *In Proceedings of the Second AES Candidate Conference, Rome, Italy, March 22–23, 1999.*

25. Chari S.; Jutla C.; Rao J.; Rohatgi P. "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards." *In Proceedings of the Second AES Candidate Conference, Rome, Italy, March 22–23, 1999.*

26. Jagger & Lewis. Available online: https://www.jagger-lewis.com/en-en/home (accessed on 21 November 2020).

27. PXI-5114 Specifications. Available online: https://www.ni.com/documentation/en/pxi-oscilloscope/latest/specs-pxi-5114/specs/ (accessed on 21 November 2020).

28. Oppenheim, A.V.; Schafer, R.W.; Buck, J.R. "Discrete-Time Signal Processing." *Prentice Hall: Upper Saddle River, NJ, USA, 1999, pp. 468-471.*