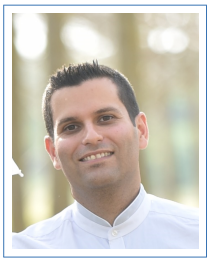
Ben Nassi, PhD

Curriculum Vitae

(+972) 54-9220091
nassiben5@gmail.com
My Webpage
Linkedin



Academic Background

2/2023 - 2/2024 **Postdoc, Cornell Tech**, *New-York*, USA.
Hosted by Prof. Thomas Ristenpart

8/2021 - 1/2023 **Postdoc, Software & Information Systems Eng.**, *Ben-Gurion University of the Negev*, Israel, Robustness of Artificial Intelligence.

10/2016- 7/2021 **Ph.D. in Software & Information Systems Eng.**, *Ben-Gurion University of the Negev*, Israel, Security and Privacy in the IoT Era (Advised by Prof. Yuval Elovici).

10/2013- 7/2015 **M.Sc. in Software & Information Systems Eng.**, *Ben-Gurion University of the Negev*, Israel, Intoxication Detection Using Internet of Wearable Things (Advised by Prof. Yuval Elovici).

10/2009- 3/2013 **B.Sc. in Computer Science**, *Ben-Gurion University of the Negev*, Israel.
Magna Cum Laude

Professional Experience

Cyber @ BGU

2023 ***Project Manager***, *Robustness of Object Detectors (with Fujitsu).*

2022 ***Project Manager***, *AI Watermarking (with Fujitsu).*

2021 ***Project Manager***, *Non-projector phantom attacks (with Toshiba).*

2020 ***Project Manager***, *Phantom Attacks against Autonomous Cars (with Toshiba).*

2019 ***Project Manager***, *New threats created by drones (with Fujitsu).*

2018 ***Project Manager***, *IoT Attack Scenarios based on IoT Future Vision (with Fujitsu).*

Google, Tel-Aviv

2016 ***SWE Internship***, *Google Cloud* .

Deutsche Telekom Innovation Labs @ BGU

2015 ***Project Manager***, *Security of SCADA systems.*

2012-2014 ***Researcher***, *Counting Pedestrians in Streets Based on call data records.*

Publications

In Conference Proceedings

2024 **Ben Nassi**, Etay Iluz, Or Cohen, Ofek Vayner, Dudi Nassi, Boris Zadov, and Yuval Elovici. Video-based cryptanalysis: Extracting cryptographic keys from video footage of a device's power led. In ***45th IEEE Symposium on Security and Privacy***, *SP 2024, San Francisco, CA, USA, 20-24 May 2024*. IEEE, 2024.

2024 Andres Fabrega, Carolina Ortega Perez, Armin Namavari, **Ben Nassi**, Rachit Agarwal, and Tom Ristenpart. Injection Attacks Against End-to-End Encrypted Applications. In ***45th IEEE Symposium on Security and Privacy***, *SP 2024, San Francisco, CA, USA, 20-24 May 2024*. IEEE, 2024.

2023 **Ben Nassi**, Ofek Vayner, Etay Iluz, Dudi Nassi, Or Hai Cohen, Jan Jancar, Daniel Genkin, Eran Tromer, Boris Zadov, and Yuval Elovici. Optical cryptanalysis: Recovering cryptographic keys from power led light fluctuations. In *CCS '23: **2023 ACM SIGSAC Conference on Computer and Communications Security***. ACM, 2023.

2022 **Ben Nassi**, Yaron Pirutin, Raz Swissa, Adi Shamir, Yuval Elovici, and Boris Zadov. Lamphone: Passive Sound Recovery from a Desk Lamp's Light Bulb Vibrations. In ***31st USENIX Security Symposium** (USENIX Security 22)*, Boston, MA, August 2022. USENIX Association.

2021 **Ben Nassi**, Yaron Pirutin, Tomer Cohen Galor, Yuval Elovici, and Boris Zadov. Glowworm Attack: Optical TEMPEST Sound Recovery via a Device's Power Indicator LED. In *CCS '21: **2021 ACM SIGSAC Conference on Computer and Communications Security**, Virtual Event, Republic of Korea, November 15 - 19, 2021*, pages 1900–1914. ACM, 2021.

2021 **Ben Nassi**, Ron Bitton, Ryusuke Masuoka, Asaf Shabtai, and Yuval Elovici. SoK: Security and Privacy in the Age of Commercial Drones. In ***42nd IEEE Symposium on Security and Privacy**, SP 2021, San Francisco, CA, USA, 24-27 May 2021*, pages 1434–1451. IEEE, 2021.

2021 **Ben Nassi**, Raz Ben-Netanel, Adi Shamir, and Yuval Elovici. Game of Drones - Detecting Spying Drones Using Time Domain Analysis. In *Cyber Security Cryptography and Machine Learning - 5th International Symposium, CSCML 2021, Be'er Sheva, Israel, July 8-9, 2021, Proceedings*, volume 12716 of *Lecture Notes in Computer Science*, pages 128–144. Springer, 2021.

2020 **Ben Nassi**, Yisroel Mirsky, Dudi Nassi, Raz Ben-Netanel, Oleg Drokin, and Yuval Elovici. Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks. In *CCS '20: **2020 ACM SIGSAC Conference on Computer and Communications Security**, Virtual Event, USA, November 9-13, 2020*, pages 293–308. ACM, 2020.

2019 **Ben Nassi**, Raz Ben-Netanel, Adi Shamir, and Yuval Elovici. Drones' Cryptanalysis - Smashing Cryptography with a Flicker. In ***2019 IEEE Symposium on Security and Privacy**, SP 2019, San Francisco, CA, USA, May 19-23, 2019*, pages 1397–1414. IEEE, 2019.

Journal & Magazine Articles

2023 **Ben Nassi**, Yisroel Mirsky, Jacob Shams, Raz Ben-Netanel, Dudi Nassi, and Yuval Elovici. Protecting autonomous cars from phantom attacks. ***Commun. ACM***, volume 66, page 56–69. Association for Computing Machinery, mar 2023.

2022 **Ben Nassi**, Jacob Shams, Lior Rokach, and Yuval Elovici. Virtual Breathalyzer: Towards the Detection of Intoxication Using Motion Sensors of Commercial Wearable Devices. ***Sensors***, volume 22, 2022.

2022 **B. Nassi**, Y. Pirutin, J. Shams, R. Swissa, Y. Elovici, and B. Zadov. Optical speech recovery from desktop speakers. *Computer*, volume 55, pages 40–51. **IEEE Computer Society**, nov 2022.

2022 Barak Davidovich, **Ben Nassi**, and Yuval Elovici. Towards the Detection of GPS Spoofing Attacks against Drones by Analyzing Camera's Video Stream. ***Sensors***, volume 22, page 2608, 2022.

2021 Raz Ben-Netanel, **Ben Nassi**, Adi Shamir, and Yuval Elovici. Detecting Spying Drones. ***IEEE Secur. Priv.***, volume 19, pages 65–73, 2021.

2019 **Ben Nassi**, Adi Shamir, and Yuval Elovici. Xerox Day Vulnerability. ***IEEE Trans. Inf. Forensics Secur.***, volume 14, pages 415–430, 2019.

2018 Alona Levy, **Ben Nassi**, Yuval Elovici, and Erez Shmueli. Handwritten Signature Verification Using Wrist-Worn Devices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, volume 2, pages 119:1–119:26, 2018.

Workshops

2023 **Ben Nassi**, Ras Swissa, Yuval Elovici, and Boris Zadov. The little seal bug: Optical sound recovery from lightweight reflective objects. In *WOOT '23: 17th IEEE Workshop on Offensive Technologies*. IEEE, 2023.

2023 Dudi Biton, Aditi Misra, Efrat Levy, Jaidip Kotak, Ron Bitton, Roei Schuster, Nicolas Papernot, Yuval Elovici, and **Ben Nassi**. The adversarial implications of variable-time inference. *In Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security (AISec '23)*, 2023.

2022 **Ben Nassi**, Jacob Shams, Raz Ben-Netanel, and Yuval Elovici. badvertisement: Attacking advanced driver-assistance systems using print advertisements. In *IEEE European Symposium on Security and Privacy, EuroS&P 2022 - Workshops, Genoa, Italy, June 6-10, 2022*, pages 376–383. IEEE, 2022.

2022 Barak Davidovich, **Ben Nassi**, and Yuval Elovici. Visas–detecting gps spoofing attacks against drones by analyzing camera's video stream. In *Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, volume 2022, page 25, 2022.

2021 **Ben Nassi**, Dudi Nassi, Raz Ben-Netanel, and Yuval Elovici. Spoofing Mobileye 630's Video Camera Using a Projector. In *Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, volume 2021, page 25, 2021.

2021 **Ben Nassi**, Aviel Levy, Yaron Pirutin, Asaf Shabtai, Ryusuke Masuoka, and Yuval Elovici. ReDroId: Remote Drone Identification Based on Visual RSA SecurID Tokens. In *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pages 1–9. IEEE, 2021.

In Peer Review & Preparation

2024 **Ben Nassi**. When photodiodes meet power leds of low-power devices: Speech eavesdropping and cryptographic keys recovery from a device's power led. *Submitted to Communications of the ACM*, 2024.

2024 **Ben Nassi**, Stav Cohen, and Ron Bitton. Compromptmized: Unleashing zero-click worms that target genai-powered applications. 2024.

2024 Jacob Shams, **Ben Nassi**, Ikuya Morikawa, Toshiya Shimizu, Asaf Shabtai, and Yuval Elovici. Seeds don't lie: An adaptive watermarking framework for computer vision models. *Submitted to CCS 24*, 2024.

2024 Armin Namavari, Barry Wang, Sanketh Menda **Ben Nassi**, Nirvan Tyagi, James Grimmelmann, Amy Zhang, and Thomas Ristenpart. Private hierarchical governance for encrypted messaging. *Submitted to SP'24*, 2024.

2024 Andres Fabrega, Carolina Ortega Perez, Armin Namavari, **Ben Nassi**, Rachit Agarwal, and Tom Ristenpart. Injection attacks against password managers. Submitted to USENIX'2024, 2024.

Additional Talks

2024 **Real World Crypto (RWC'24)**, *Toronto, Canada*, Extracting Secret Keys from a Device's Power LED using COTS Video Cameras..

2023 **BlackHat Europe 23**, *London, UK*, Indirect Prompt Injection into LLMs using Images and Sounds.

2023 **SecTor 23**, *Toronto, Canada*, Video-Based Cryptanalysis: Recovering Cryptographic Keys from Non-compromised Devices Using Video Footage of a Device's Power LED.

2023 **DEFCON 31**, *Las-Vegas, USA*, Video-Based Cryptanalysis: Recovering Cryptographic Keys from Non-compromised Devices Using Video Footage of a Device's Power LED.

2023 **BlackHat USA 23**, *Las-Vegas, USA*, Video-Based Cryptanalysis: Recovering Cryptographic Keys from Non-compromised Devices Using Video Footage of a Device's Power LED.

2023 **CyberWeek 23**, *Security and Safety in the Era of Autonomous Cars*, TAU, Israel.

2022 **BlackHat Asia 22**, *Singapore*, The Little Seal Bug: Optical Sound Recovery from Lightweight Reflective Objects.

2022 **AI Week 22**, *Remote Split-second Phantom Attacks on AI of Semi & full Autonomous Cars*.

2021 **HITB+CyberWeek 21**, *UAE*, Towards Eletro-Optical Sound Eavesdropping.

2021 **SecTor 21**, *Canada*, Detecting Illicit Drone Filming.

2021 **SecTor 21**, *Canada*, Ghost Misdetection Attacks Against Tesla Model X & Mobileye 630 PRO.

2021 **Car Hacking Village @ DEFCON 29**, *USA*, Remote Adversarial Phantom Attacks on Tesla & Mobileye.

2021 **RSA Conference 21**, *USA*, Securing Tesla & Mobileye from Split-Second Phantom Attacks.

2021 **BlackHat Asia 21**, *The Motion Sensor Western: The Good (Automatic Functionality Support), the Bad (Security Risks to Devices), and the Ugly (Privacy Risks to Individuals)*.

2020 **CodeBlue 20**, *Japan*, Drones Cryptanalysis: Detecting Spying Drones.

2020 **CodeBlue 20**, *Japan*, Lamphone: Real Time Passive Sound Recovery from Vibration of a Hanging Light Bulb.

2020 **SecTor 20**, *Canada*, Lamphone: Real Time Passive Sound Recovery from Vibration of a Hanging Light Bulb.

2020 **BlackHat 20**, *USA*, Lamphone: Real Time Passive Sound Recovery from Vibration of a Hanging Light Bulb.

2020 **CyberTech TLV 20**, *Phantom of the ADAS*.

2020 **RSA Conference 20**, *USA*, Air-Gapping Is Overrated: Pressing a Red-Button via a Multifunction Printer.

2018 **IoT Village @ DEFCON 26**, *USA*, Attacking Smart Irrigation Systems.

Invited Seminars

2024 **Seminar @ CS, Boston University**, *USA*, Extracting Secret Keys from a Device's Power LED using COTS Video Cameras..

2024 **Seminar @ CS, MIT**, *USA*, Extracting Secret Keys from a Device's Power LED using COTS Video Cameras..

2023 **Seminar @ CS, Stanford**, *USA*, Video-Based Cryptanalysis: Recovering Cryptographic Keys from Non-compromised Devices Using Video Footage of a Device's Power LED.

2023 **Seminar @ CISPA**, *Germany*, Video-Based Cryptanalysis: Recovering Cryptographic Keys from Non-compromised Devices Using Video Footage of a Device's Power LED.

2023 **Seminar @ CS, Columbia University**, *USA*, When Optical Sensors Meet Low-Power Devices: Recovering Speech and Cryptographic Keys from Light Emitted from Power LEDs and Light Bulbs.

2023 **Seminar @ CS, HUJI**, *Israel*, When Optical Sensors Meet Low-Power Devices: Recovering Speech and Cryptographic Keys from Light Emitted from Power LEDs and Light Bulbs.

2023 **Seminar @ EE, Tel-Aviv University**, *Israel*, When Optical Sensors Meet Low-Power Devices: Recovering Speech and Cryptographic Keys from Light Emitted from Power LEDs and Light Bulbs.

2022 **Seminar @ CE Club, Technion**, *Israel*, Finding Darkness in the Light: Recovering Speech and Cryptographic keys from Light Emitted from Power LEDs and Light Bulbs..

2022 **Seminar @ Michigan State University**, *Towards Electro-optical Sound Eavesdropping*.

2021 **Seminar @ Cornell Tech**, *Towards Electro-optical Sound Eavesdropping*.

2021 **Seminar @ Ben-Gurion University of the Negev**, *Security & Privacy in the IoT Era*.

2021 **8th Privacy, Cyber and Technology Workshop**, *Detecting A Drone's Illicit Video Streaming*.

2020 **Seminar @ HUJI**, *Phantom of the ADAS*.

Patents

Granted

2021 **Ben Nassi**, Adi Shamir, and Yuval Elovici. Analyzing radio transmission for detecting whether a drone is filming a point of interest. 2021.

2019 **Ben Nassi**, Yuval Elovici, Erez Shmueli, and Alona Levy. A method for online signature verification using wrist-worn devices. 2019.

Pending

2023 Ben Nassi, Yuval Elovici, Yisroel Avraham Mirsky, Dudi Nassi, and Raz Ben Nethanel. Methods for detecting phantom projection attacks against computer vision algorithms. 2023.

Fellowships & Awards

2023 **Pwnie Award** for The Best Cryptographic Attack of 2023 for Video-based Cryptanalysis

2023 **Viterbi Fellowship** for Nurturing Future Faculty Members (by ECE, Technion).

2023 **Tim Höttges Award in Cybersecurity Research** for Optical Cryptanalysis - $2,500

2022 **Urban Tech Hub Fellowship** for postdoctoral researchers, Jacobs Technion-Cornell Institute, Cornell Tech.

2022 **BGU Dean Award for excellence in Ph.D**, Ben-Gurion University of the Negev

2021 **Best Demo Award** for Phantom of the ADAS by AutoSec'21

2020 Runner up for **Pwnie Award** for The Most Innovative Research 2020 for Lamphone

2020 Runner up for **Pwnie Award** for The Most Epic Achievement 2020 for Lamphone

2020 Runner up for **CSAW'20** for Lamphone

2020 Runner up for **CSAW'20** for Phantom of the ADAS

2019 Runner up for **CSAW'19** for Drones Cryptanalysis

2018 –2021 **Mid. Way Negev-Faran Scholarship for Excellence Ph.D Program**, Kreitman School of Advanced Graduate Studies, Ben-Gurion University of the Negev.

Professional Activity

2024 **Review Board** in ***BlackHat-Asia* 2024**, Singapore.

2023 **Review Board** in ***BlackHat-Europe* 2023**, London, England.

2023 **PC Member** in ***Workshop On Offensive Technologies (WOOT) 2023*, San Francisco, USA**

2023 **PC Member** in ***The ACM Conference on Computer and Communications Security (CCS)* 2023**, Copenhagen, Denmark.

2023 **Review Board** in ***BlackHat-Asia* 2023**, Singapore.

2022 **Review Board** in ***BlackHat-Europe* 2022**, London, England.

2022 **PC Member** in ***The ACM Conference on Computer and Communications Security (CCS)* 2022**, Los Angeles, USA.

2022 **PC Member** in ***Fourth International Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022***, San Diego, USA.

2020 **Student PC Member** in ***IEEE Symposium on Security and Privacy* 2020**, San-Francisco, USA.

2019 **Student PC Member** in ***IEEE Symposium on Security and Privacy* 2019**, San-Francisco, USA.

Media Attention

- **TV Interviews & Podcasts** *London & Kirshenbaum*, *Lama Cyber-1?*, *Lama Cyber-2?*
- **Video-based Cryptanalysis** was covered by *ArsTechnica*, *Forbes*, *The Hacker News*, *The Byte*, *HackRead*, *Hackster*, *Kaspersky*,
- **Lamphone** was covered by *Forbes*, *Wired*, *Fox News*, *India Times*, *Kaspersky Daily*, *Threat Post*, *The Hacker News*, *ZDNet Security Affairs*, *GB Hackers*, *Popular Mechanics*, *Digital Trends*, *Saudi Expatriate*, *Hack Read*, *PC Mag*, *Naked Security*
- **Drones Cryptanalysis** was covered by *Wired*, *Eurek Alert*, *Globes*, *JPost*, *Science Daily*, *Science News Explores*, *Ynet*
- **Phantom of the ADAS** was covered by *Wired*, *Ars Technica*, *Kaspersky Daily*, *Popular Mechanics*, *The Next Web*, *Threat Post*, *Security Affairs*, *Car and Driver*, *Jpost*, *Driving*, *Bank Info Security*, *Tech Xplore*, *Interesting Engineering*,
- **The Glowworm Attack** was covered by *Forbes*, *Ars Technica*, *Threat Post*, *The Hacker News*, *All About Circuits*, *Review Geek*, Security Affairs, *Exec Security*, *Interesting Engineering*, *Commercial Integrator*, *Gizmodo*, *AV Magazine*
- **Virtual Breathalyzer** was covered by *Mirror*, *Insider*, *The Christian Science Monitor*, *The Times of Israel*, *No Camels*, *Vocativ*.
- **Piping Botnet** was covered by *Motherboard*, *MIT Technology Review*, *Security Affairs*, *We Live Security*, *Security Week*, *MSSP Alert*.
- **The Little Seal Bug Attack** was covered by *Wired*, *Top Tech*, *The Shock News*, *Global News*
- **Xerox Day Vulnerability** was covered by *Motherboard*, *Communication of the ACM*, *Phys*, *Science Daily No Camels*

Teaching Assistantship

Spring, 2021 **Introduction to network and computer security**, *Ben-Gurion University of the Negev*.
Spring, 2020 **Introduction to network and computer security**, *Ben-Gurion University of the Negev*.
Spring, 2019 **Introduction to network and computer security**, *Ben-Gurion University of the Negev*.
Spring, 2018 **Introduction to network and computer security**, *Ben-Gurion University of the Negev*.

Advising

M.Sc. Students

2021-Present ***Ofek Vayner***, *Optical Cryptanalysis: Recovering Secret Keys using a Photodiode*.
2021-Present ***Dudi Biton***, *Timing Based Adversarial Attacks*.
2021-Present ***Jacob Shams***, *Adaptive watermarking framework for neural networks*.
2021-Present ***Elad Feldman***, *Securing advanced driving assistance systems from epileptic syndrome*.
2020-2022 ***Barak Davidovich***, *Detecting GPS spoofing attacks against drones via video stream analysis*.
2019-2021 ***Raz Ben Netanel***, *Detecting illicit video filming*.

Undergraduate Students

2021-Present ***Etay Iluz***, *Video-based Cryptanalysis: Recovering Secret Keys using Video Cameras*.
2020-Present ***Raz Swissa***, *Real Time Passive Sound Recovery from Shiny Lightweight Objects*.
2020 ***Dudi Nassi***, *Phantom attacks on autonomous cars*.
2019-2021 ***Yaron Pirutin***, *Real Time Passive Sound Recovery from Vibration of a Hanging Light Bulb*.
2018-2020 ***Aviel Levy***, *Remote Optical Drone Authentication*.
2018-2020 ***Idan Sokolovsky***, *Real Time Passive Sound Recovery from Vibration of a Privacy Shield*.
2017-2018 ***David Hirschman***, *Real Time Passive Sound Recovery from Vibration of a Privacy Shield*.
2017-2018 ***Hido Cohen***, *Biological Covert Channels*.

2017-2018 ***Moshe Sror***, *Cyberattacks against commercial smart irrigation systems.*

High-School Students (Magshimim Project)

2021 ***Tomer Galor***, *Real Time Passive Sound Recovery from a Device's Power Indicator LED.*

2019 ***Ruslan Veremyenko***, *Cyberattacks against commercial smart irrigation systems.*

2018 ***Roei Cohen***, *Security of Drones.*

2018 ***Ido Lavi***, *Cyberattacks against commercial smart irrigation systems.*

2017 ***Aviv Barel***, *Establishing a Covert Channel via MFP.*