the hardware hacking handbook

The Hardware Hacking Handbook: A Deep Dive into the World of Tinkering

the hardware hacking handbook is more than just a guide—it’s a gateway for enthusiasts, engineers, and curious minds who want to explore the inner workings of electronic devices. Whether you’re a beginner eager to learn how to modify gadgets or a seasoned professional aiming to expand your knowledge on embedded systems, this handbook offers a treasure trove of techniques, insights, and practical advice. Hardware hacking is a fascinating blend of creativity, problem-solving, and technical skill, and this handbook invites you into that world with open arms.

Understanding the Basics of Hardware Hacking

Before diving into the complexities of circuits and microcontrollers, it’s essential to grasp what hardware hacking truly means. At its core, hardware hacking involves examining, modifying, and sometimes repurposing physical electronic devices to unlock new functionalities or to better understand their design.

What Is Hardware Hacking?

Hardware hacking is the art of exploring the physical components of electronic devices. Unlike software hacking, which manipulates code, hardware hacking delves into the tangible parts—circuit boards, chips, sensors, and more. It can range from simple modifications like adding a custom LED to advanced techniques such as reverse engineering firmware or bypassing security measures.

Why the Hardware Hacking Handbook Matters

The hardware world is vast and often intimidating, especially for newcomers. The hardware hacking handbook serves as a roadmap, breaking down complex concepts into digestible sections. It covers everything from soldering basics to advanced debugging tools, empowering readers to tackle real-world projects confidently.

Essential Tools and Equipment for Hardware

Hacking

No hardware hacker can succeed without the right tools. The handbook meticulously details the must-have equipment for anyone serious about tinkering with electronics.

Basic Toolkit for Beginners

Getting started doesn’t require an extravagant setup. Here’s a list of foundational tools emphasized in the hardware hacking handbook:

- **Soldering Iron:** For assembling and modifying circuits.
- **Multimeter:** To measure voltage, current, and resistance.
- **Wire Strippers and Cutters:** Essential for preparing wires.
- **Breadboard:** For prototyping without soldering.
- **Basic Hand Tools:** Screwdrivers, tweezers, and pliers.

Advanced Tools for Deep Dives

As your skills grow, the hardware hacking handbook introduces more sophisticated tools:

- **Logic Analyzers:** To capture and analyze digital signals.
- **Oscilloscopes:** For observing waveform signals in circuits.
- **JTAG and SPI Debuggers:** To interface directly with chips.
- **Firmware Dumpers:** Devices to extract firmware from embedded chips.

Core Techniques Explored in the Hardware Hacking Handbook

The beauty of hardware hacking lies in its variety of techniques, each

unlocking different layers of a device's functionality.

Reverse Engineering Hardware

One of the most exciting aspects detailed in the hardware hacking handbook is reverse engineering. This process involves deconstructing a device to understand how it operates internally. Techniques include:

- Analyzing circuit schematics and layouts.
- Tracing signal paths on printed circuit boards (PCBs).
- Using microscopes to inspect microchips and solder joints.

Reverse engineering is crucial for security research, repair, and creating compatible accessories.

Firmware Extraction and Modification

Firmware acts as the brain of many devices, controlling hardware behavior at a fundamental level. The handbook guides readers through safely extracting firmware using hardware debuggers or chip readers. It also explains how to analyze and patch firmware to add features or fix vulnerabilities.

Signal Analysis and Protocol Sniffing

Understanding communication protocols—such as I2C, SPI, UART—is vital for hardware hackers. The hardware hacking handbook covers how to intercept and decode these signals, enabling you to interact with devices more effectively and potentially unlock hidden functionalities.

Safety and Ethical Considerations in Hardware Hacking

While hardware hacking opens many exciting avenues, it’s essential to approach it responsibly. The handbook emphasizes safety—both physical and legal.

Physical Safety Tips

Working with electronics involves risks like electric shocks, burns, or damaging expensive equipment. The handbook suggests:

- Always unplug devices before disassembly.
- Use anti-static wristbands to prevent electrostatic discharge (ESD).
- Maintain a well-ventilated workspace when soldering.

Legal and Ethical Boundaries

Not all hardware hacking is legal or ethical. The handbook encourages understanding local laws about device modification and respecting intellectual property rights. It also advocates for responsible disclosure when discovering security flaws, helping to improve overall device safety.

Learning from Real-World Hardware Hacking Projects

One of the most compelling features of the hardware hacking handbook is its inclusion of practical projects that demonstrate concepts in action. These projects help readers apply their knowledge and build confidence.

Modifying Consumer Electronics

Examples include adding custom lighting to gaming consoles or tweaking smart home devices to extend their capabilities. Such projects teach soldering, firmware flashing, and protocol analysis.

Building Custom Gadgets

The handbook also guides readers through building devices from scratch using microcontrollers like Arduino or Raspberry Pi. This hands-on approach fosters creativity and a deeper understanding of electronics fundamentals.

Repair and Restoration

Another valuable application is reviving broken electronics. By diagnosing faults and replacing components, hardware hackers can save money and reduce electronic waste—a win for both hobbyists and the environment.

Expanding Your Hardware Hacking Skills Beyond the Handbook

The hardware hacking handbook is a fantastic starting point, but the journey doesn’t end there. Learning is ongoing in this rapidly evolving field.

Joining Communities and Forums

Engaging with online communities, such as Reddit’s r/hardwarehacking or specialized forums, provides access to collective knowledge, troubleshooting help, and collaboration opportunities.

Attending Workshops and Conferences

Events like DEF CON, HOPE, or local maker fairs offer hands-on workshops and networking chances with experienced hackers and professionals.

Keeping Up with Latest Tools and Techniques

Technology changes fast. Following blogs, YouTube channels, and subscribing to newsletters focused on hardware security and hacking ensures you stay updated on new methodologies and tools.

The hardware hacking handbook serves as a comprehensive foundation that opens the door to endless possibilities in understanding and manipulating electronic devices. Whether your goal is to innovate, repair, or simply learn, this resource is an invaluable companion on your hardware hacking journey.

Frequently Asked Questions

What is 'The Hardware Hacking Handbook' about?

'The Hardware Hacking Handbook' is a comprehensive guide that covers techniques and tools for analyzing, reverse engineering, and hacking hardware devices, aimed at security researchers and enthusiasts.

Who are the authors of 'The Hardware Hacking Handbook'?

The book is authored by Jasper van Woudenberg and Colin O'Flynn, both well-known experts in hardware security and embedded systems.

What topics are covered in 'The Hardware Hacking Handbook'?

The handbook covers hardware reverse engineering, side-channel attacks, fault injection, embedded device analysis, debugging techniques, and security assessment methods.

Is 'The Hardware Hacking Handbook' suitable for beginners?

While the book is accessible, it is primarily geared toward readers with some prior knowledge of electronics and security concepts, though beginners can benefit with additional background study.

Does 'The Hardware Hacking Handbook' include practical examples?

Yes, the book provides numerous practical examples, hands-on exercises, and case studies to illustrate hardware hacking techniques in real-world scenarios.

What tools are recommended in 'The Hardware Hacking Handbook'?

The handbook discusses a variety of hardware hacking tools such as oscilloscopes, logic analyzers, JTAG debuggers, glitching devices, and open-source software for analysis.

How does 'The Hardware Hacking Handbook' help with hardware security testing?

It provides methodologies and step-by-step approaches to identify vulnerabilities in hardware, enabling security professionals to perform thorough hardware security assessments.

Where can I purchase 'The Hardware Hacking Handbook'?

The book is available for purchase on major online retailers like Amazon, as well as directly from the publisher's website and selected technical bookstores.

Additional Resources

The Hardware Hacking Handbook: A Detailed Exploration of Practical Electronics Security

the hardware hacking handbook emerges as a seminal resource for enthusiasts, professionals, and security researchers invested in the domain of embedded systems and electronic device security. With the proliferation of Internet of Things (IoT) devices and the escalating complexity of hardware architectures, understanding vulnerabilities at the hardware level has never been more crucial. This handbook offers a methodical approach to dissecting, analyzing, and manipulating hardware components, providing an essential knowledge base for those seeking to explore the intersection of physical electronics and cybersecurity.

Understanding the Scope of The Hardware Hacking Handbook

Unlike software-centric security guides, the hardware hacking handbook delves into the tangible aspects of security breaches—those that require interaction beyond code. It covers a spectrum of techniques ranging from simple circuit probing to sophisticated fault injections and side-channel attacks. The book situates itself uniquely by balancing theoretical frameworks with hands-on methodologies, making it accessible to both novices and seasoned practitioners in hardware security.

The handbook’s relevance is amplified by the current technology landscape. With billions of connected devices worldwide, hardware vulnerabilities pose significant risks, often overlooked in favor of software defenses. The hardware hacking handbook addresses this gap by emphasizing the importance of physical security assessments and reverse engineering, highlighting how attackers can exploit hardware weaknesses to undermine entire systems.

Key Themes and Techniques Explored

A core strength of the hardware hacking handbook lies in its comprehensive coverage of diverse hardware hacking techniques. These include:

- **Reverse Engineering:** Detailed procedures for extracting schematics, understanding integrated circuits (ICs), and analyzing printed circuit boards (PCBs).
- **Debugging Interfaces:** Utilization of JTAG, UART, and SPI interfaces to gain low-level access to device internals.
- **Fault Injection:** Methods such as voltage glitching and clock manipulation to induce erroneous behavior in hardware.
- **Side-Channel Analysis:** Techniques to glean sensitive information by monitoring power consumption, electromagnetic emissions, or timing variations.
- **Firmware Extraction and Modification:** Strategies for dumping, analyzing, and altering firmware to understand device behavior or implement custom functionality.

These themes are not only discussed conceptually but are supplemented with practical examples, hardware tool recommendations, and troubleshooting tips, reinforcing the handbook’s utility as a field guide.

Comparative Perspective: How The Hardware Hacking Handbook Stands Out

When compared to other security manuals focusing on software or network vulnerabilities, the hardware hacking handbook fills a niche that is often underserved. For instance, while books like “The Web Application Hacker’s Handbook” or “Practical Malware Analysis” provide deep dives into their respective fields, they rarely touch upon hardware intricacies. The hardware hacking handbook complements these by addressing the foundational layer of physical devices.

Furthermore, unlike highly technical datasheets or fragmented online tutorials, this handbook consolidates knowledge into a coherent framework. It is structured to gradually build the reader’s proficiency, starting with basic soldering and multimeter use, advancing to advanced cryptographic chip attacks. This pedagogical approach facilitates skill acquisition without overwhelming newcomers.

Tools and Resources Highlighted

The handbook also extensively discusses essential hardware hacking tools, which cater to various skill levels and budgets. Some notable mentions

include:

1. **Oscilloscopes and Logic Analyzers:** For capturing and interpreting signal behaviors.
2. **Microcontroller Development Boards:** Such as Arduino and Raspberry Pi, used for prototyping and interfacing.
3. **Chip-Off Equipment:** Tools for physically removing memory chips to extract data.
4. **Programming and Debugging Interfaces:** Devices like Bus Pirate and JTAGulator that facilitate communication with hardware components.
5. **Software Suites:** Open-source tools like IDA Pro (for firmware analysis) and Chipsec (for hardware security assessment).

By providing detailed overviews and use cases for these tools, the hardware hacking handbook serves as a practical manual not only for understanding theory but also for applying it in real-world scenarios.

The Educational Value and Limitations

The pedagogical merit of the hardware hacking handbook cannot be overstated. Its clear explanations, accompanied by schematics and photographs, enable self-paced learning. The inclusion of ethical considerations and legal boundaries also demonstrates responsible guidance, which is critical given the sensitive nature of hardware exploitation.

However, it is important to acknowledge some limitations. The rapid evolution of hardware technologies means that certain specific device examples or attack vectors may become outdated. Readers should supplement the handbook with current research papers and community forums to stay updated on emerging threats and techniques.

Additionally, mastering hardware hacking demands patience and hands-on experimentation, which the book encourages but cannot fully substitute. Access to specialized equipment can also pose a barrier for some readers, although the handbook’s coverage of low-cost tools partially mitigates this challenge.

Integrating The Hardware Hacking Handbook into

Professional Practice

For security professionals, the hardware hacking handbook represents an invaluable asset to diversify their skill set. Incorporating hardware vulnerability assessments into existing security audits enhances overall threat detection and mitigation strategies. Organizations dealing with critical infrastructure or consumer electronics stand to benefit from the insights provided, particularly in identifying supply chain risks and counterfeit components.

Moreover, educators in cybersecurity and electronics engineering programs can leverage the handbook's structured content to design curricula that address an often-neglected segment of security education. Its practical approach aligns well with laboratory exercises and project-based learning.

In the realm of hobbyists and makers, the handbook inspires innovation by revealing hidden potentials of everyday hardware. It encourages experimentation that can lead to novel applications or improved device designs, fostering a community of informed and skilled practitioners.

The hardware hacking handbook, through its detailed exposition and practical guidance, underscores the importance of hardware security in the broader cybersecurity landscape. By demystifying complex concepts and offering actionable insights, it contributes significantly to cultivating a deeper understanding of how physical device vulnerabilities can be identified and mitigated.

The Hardware Hacking Handbook

the hardware hacking handbook: *The Hardware Hacking Handbook* Jasper van Woudenberg, Colin O'Flynn, 2021-12-21 The Hardware Hacking Handbook takes you deep inside embedded devices to show how different kinds of attacks work, then guides you through each hack on real hardware. Embedded devices are chip-size microcomputers small enough to be included in the structure of the object they control, and they're everywhere—in phones, cars, credit cards, laptops, medical equipment, even critical infrastructure. This means understanding their security is critical. The Hardware Hacking Handbook takes you deep inside different types of embedded systems, revealing the designs, components, security limits, and reverse-engineering challenges you need to know for executing effective hardware attacks. Written with wit and infused with hands-on lab experiments, this handbook puts you in the role of an attacker interested in breaking security to do good. Starting with a crash course on the architecture of embedded devices, threat modeling, and attack trees, you'll go on to explore hardware interfaces, ports and communication protocols,

electrical signaling, tips for analyzing firmware images, and more. Along the way, you'll use a home testing lab to perform fault-injection, side-channel (SCA), and simple and differential power analysis (SPA/DPA) attacks on a variety of real devices, such as a crypto wallet. The authors also share insights into real-life attacks on embedded systems, including Sony's PlayStation 3, the Xbox 360, and Philips Hue lights, and provide an appendix of the equipment needed for your hardware hacking lab – like a multimeter and an oscilloscope – with options for every type of budget. You'll learn: How to model security threats, using attacker profiles, assets, objectives, and countermeasures Electrical basics that will help you understand communication interfaces, signaling, and measurement How to identify injection points for executing clock, voltage, electromagnetic, laser, and body-biasing fault attacks, as well as practical injection tips How to use timing and power analysis attacks to extract passwords and cryptographic keys Techniques for leveling up both simple and differential power analysis, from practical measurement tips to filtering, processing, and visualization Whether you're an industry engineer tasked with understanding these attacks, a student starting out in the field, or an electronics hobbyist curious about replicating existing work, The Hardware Hacking Handbook is an indispensable resource – one you'll always want to have onhand.

the hardware hacking handbook: The Hardware Hacking Handbook Colin O'Flynn, 2021 Embedded devices are chip-size microcomputers small enough to be included in the structure of the object they control, and they're everywhere-in phones, cars, credit cards, laptops, medical equipment, even critical infrastructure. This means understanding their security is critical. The Hardware Hacking Handbook takes you deep inside different types of embedded systems, revealing the designs, components, security limits, and reverse-engineering challenges you need to know for executing effective hardware attacks. Written with wit and infused with hands-on lab experiments, this handbook puts you in the role of an attacker interested in breaking security to do good. Starting with a crash course on the architecture of embedded devices, threat modeling, and attack trees, you'll go on to explore hardware interfaces, ports and communication protocols, electrical signaling, tips for analyzing firmware images, and more. Along the way, you'll use a home testing lab to perform fault-injection, side-channel (SCA), and simple and differential power analysis (SPA/DPA) attacks on a variety of real devices, such as a crypto wallet. The authors also share insights into real-life attacks on embedded systems, including Sony's PlayStation 3, the Xbox 360, and Philips Hue lights, and provide an appendix of the equipment needed for your hardware hacking lab - like a multimeter and an oscilloscope - with options for every type of budget. You'll learn: •How to model security threats, using attacker profiles, assets, objectives, and countermeasures •Electrical basics that will help you understand communication interfaces, signaling, and measurement •How to identify injection points for executing clock, voltage, electromagnetic, laser, and body-biasing fault attacks, as well as practical injection tips •How to use timing and power analysis attacks to extract passwords and cryptographic keys •Techniques for leveling up both simple and differential power analysis, from practical measurement tips to filtering, processing, and visualization Whether you're an industry engineer tasked with understanding these attacks, a student starting out in the field, or an electronics hobbyist curious about replicating existing work, The Hardware Hacking Handbook is an indispensable resource - one you'll always want to have onhand.

the hardware hacking handbook: The Hardware Hacking Handbook Jasper van Woudenberg, Colin O'Flynn, 2021-12-21 The Hardware Hacking Handbook takes you deep inside embedded devices to show how different kinds of attacks work, then guides you through each hack on real hardware. Embedded devices are chip-size microcomputers small enough to be included in the structure of the object they control, and they're everywhere—in phones, cars, credit cards, laptops, medical equipment, even critical infrastructure. This means understanding their security is critical. The Hardware Hacking Handbook takes you deep inside different types of embedded systems, revealing the designs, components, security limits, and reverse-engineering challenges you need to know for executing effective hardware attacks. Written with wit and infused with hands-on lab experiments, this handbook puts you in the role of an attacker interested in breaking security to do good. Starting with a crash course on the architecture of embedded devices, threat modeling, and

attack trees, you'll go on to explore hardware interfaces, ports and communication protocols, electrical signaling, tips for analyzing firmware images, and more. Along the way, you'll use a home testing lab to perform fault-injection, side-channel (SCA), and simple and differential power analysis (SPA/DPA) attacks on a variety of real devices, such as a crypto wallet. The authors also share insights into real-life attacks on embedded systems, including Sony's PlayStation 3, the Xbox 360, and Philips Hue lights, and provide an appendix of the equipment needed for your hardware hacking lab – like a multimeter and an oscilloscope – with options for every type of budget. You'll learn: How to model security threats, using attacker profiles, assets, objectives, and countermeasures Electrical basics that will help you understand communication interfaces, signaling, and measurement How to identify injection points for executing clock, voltage, electromagnetic, laser, and body-biasing fault attacks, as well as practical injection tips How to use timing and power analysis attacks to extract passwords and cryptographic keys Techniques for leveling up both simple and differential power analysis, from practical measurement tips to filtering, processing, and visualization Whether you're an industry engineer tasked with understanding these attacks, a student starting out in the field, or an electronics hobbyist curious about replicating existing work, The Hardware Hacking Handbook is an indispensable resource – one you'll always want to have onhand.

the hardware hacking handbook: *Hardware Hacking* Joe Grand, Kevin D. Mitnick, Ryan Russell, 2004-01-29 If I had this book 10 years ago, the FBI would never have found me! -- Kevin Mitnick This book has something for everyone---from the beginner hobbyist with no electronics or coding experience to the self-proclaimed gadget geek. Take an ordinary piece of equipment and turn it into a personal work of art. Build upon an existing idea to create something better. Have fun while voiding your warranty! Some of the hardware hacks in this book include: * Don't toss your iPod away when the battery dies! Don't pay Apple the $99 to replace it! Install a new iPod battery yourself without Apple's help* An Apple a day! Modify a standard Apple USB Mouse into a glowing UFO Mouse or build a FireWire terabyte hard drive and custom case* Have you played Atari today? Create an arcade-style Atari 5200 paddle controller for your favorite retro videogames or transform the Atari 2600 joystick into one that can be used by left-handed players* Modern game systems, too! Hack your PlayStation 2 to boot code from the memory card or modify your PlayStation 2 for homebrew game development* Videophiles unite! Design, build, and configure your own Windows- or Linux-based Home Theater PC* Ride the airwaves! Modify a wireless PCMCIA NIC to include an external antenna connector or load Linux onto your Access Point* Stick it to The Man! Remove the proprietary barcode encoding from your CueCat and turn it into a regular barcode reader* Hack your Palm! Upgrade the available RAM on your Palm m505 from 8MB to 16MB· Includes hacks of today's most popular gaming systems like Xbox and PS/2.· Teaches readers to unlock the full entertainment potential of their desktop PC.· Frees iMac owners to enhance the features they love and get rid of the ones they hate.

the hardware hacking handbook: Getting Started with FPGAs Russell Merrick, 2023-11-21 Skip the complexity and learn to program FPGAs the easy way through this hands-on, beginner-friendly introduction to digital circuit design with Verilog and VHDL. Whether you have been toying with field programmable gate arrays (FPGAs) for years or are completely new to these reprogrammable devices, this book will teach you to think like an FPGA engineer and develop reliable designs with confidence. Through detailed code examples, patient explanations, and hands-on projects, Getting Started with FPGAs will actually get you started. Russell Merrick, creator of the popular blog Nandland.com, will guide you through the basics of digital logic, look-up tables, and flip-flops, as well as high-level concepts like state machines. You'll explore the fundamentals of the FPGA build process including simulation, synthesis, and place and route.You'll learn about key FPGA primitives, such as DSP blocks and PLLs, and examine how FPGAs handle math operations and I/O. Code examples are provided in both Verilog and VHDL, making the book a valuable resource no matter your language of choice. You'll discover how to: Implement common design building blocks like multiplexers, LFSRs, and FIFOs Cross between clock domains without triggering metastable conditions or timing errors Avoid common pitfalls when performing math Transmit and

receive data at lightning speeds using SerDes Write testbench code to verify your designs are working With this accessible, hands-on guide, you'll be creating your own functional FPGA projects in no time. Getting started with FPGAs has never been easier.

the hardware hacking handbook: Engineering Secure Devices Dominik Merli, 2024-07-23 This practical guide to building embedded and IoT devices securely is an essential resource for current and future developers tasked with protecting users from the potential threats of these ubiquitous devices. As an engineer, you know that countless devices—from industrial components to smart household appliances—rely on embedded computer systems. But how do you balance the need for robust security with performance and innovative product design? Engineering Secure Devices will guide you through crafting secure devices—from protecting crucial assets to the nature of attackers and the risks they pose. You'll explore the technical intricacies and pros and cons of symmetric and asymmetric cryptography and learn how to use and analyze random number generators and cryptographic algorithms. You'll learn how to ensure confidential data storage and secure memory, and devise secure device identity solutions and communication protocols to reinforce system architecture against potential threats. And finally, you'll learn how to properly design secure boot and secure update processes, manage access control, and perform system monitoring to secure IoT devices. Real-world case studies throughout highlight practical applications, solutions, and obstacles, such as firmware updates with SWUpdate, secure communication with MQTT, and advanced access control with AppArmor. You'll also dig into topics like: Analyzing the performance of cryptographic implementations in both hardware and software Considerations for secure boot and software update processes to ensure ongoing firmware integrity Designing robust device architectures that withstand attacks while maintaining critical operations Developing strategies to detect and respond to anomalies or security breaches in embedded systems Whether you're an IoT developer or an embedded system architect, Engineering Secure Devices equips you with the indispensable knowledge to design, secure, and support the next generation of smart devices—from webcams to four-legged robots.

the hardware hacking handbook: From Day Zero to Zero Day Eugene Lim, 2025-08-12 Find vulnerabilities before anyone else does. Zero days aren't magic—they're missed opportunities. From Day Zero to Zero Day teaches you how to find them before anyone else does. In this hands-on guide, award-winning white-hat hacker Eugene "Spaceraccoon" Lim breaks down the real-world process of vulnerability discovery. You'll retrace the steps behind past CVEs, analyze open source and embedded targets, and build a repeatable workflow for uncovering critical flaws in code. Whether you're new to vulnerability research or sharpening an existing skill set, this book will show you how to think—and work—like a bug hunter. You'll learn how to: Identify promising targets across codebases, protocols, and file formats. Trace code paths with taint analysis and map attack surfaces with precision. Reverse engineer binaries using Ghidra, Frida, and angr. Apply coverage-guided fuzzing, symbolic execution, and variant analysis. Build and validate proof-of-concept exploits to demonstrate real-world impact. More than a toolkit, this is a window into how top vulnerability researchers approach the work. You'll gain not just techniques but also the mindset to go deeper, ask better questions, and find what others miss. If you're ready to stop reading write-ups and start writing them, From Day Zero to Zero Day is your guide.

the hardware hacking handbook: Locksport Jos Weyers, Matt Burrough, Walter Belgers, BandEAtoZ, Nigel Tolley, 2024-03-19 A comprehensive, fully illustrated guide to the fascinating sport of picking locks, Locksport is authored by five of the field's foremost champions. Together, they'll show you how to ethically, efficiently, and effectively bypass anything—from simple locks and safe dials to deadlocks and vaults. Welcome to the world of locksport, the sport of defeating locks. Whether you're new to the challenge of lockpicking or aiming for championship gold, this book serves as your definitive guide, packed with practical advice from a team of experts. DIVE INTO THE ESSENTIALS WITH LOCKSPORT FOUNDATIONS How various locks work and how to maintain and disassemble practice locks What makes some locks more secure than others The laws, competitions, and communities that make up the world of locksport MASTER YOUR CRAFT WITH HANDS-ON

TECHNIQUES How to pick pin tumblers and lever locks, make impressions or craft a working key from a blank, and manipulate open combination safe locks How to work with picks, rakes, tension wrenches, files, magnification tools, safe-lock graphs, and depth-measuring instruments The intricacies of security pins, wards, dimple locks, keyways, and antique locks GAIN THE COMPETITIVE EDGE WITH COMPETITION INSIGHTS The ins and outs of competition setup and tools and how to host your own competitions Expert strategies for managing your nerves and gathering lock intel What it's like to participate in timed head-to-head competitions, PicTacToe™, escape challenges, and other lockpicking contests From mastering your first padlock to conquering a competition, Locksport will show you how to take your skills to the next level—and have endless fun doing it.

the hardware hacking handbook: Arduino for Arduinians John Boxall, 2023-10-24 Guided by an expert craftsman with over 30 years of experience, you'll build 70 awesome Arduino projects and emerge a true Arduinian ready to invent your own complex creations. For Arduino programmers who've mastered the basics, this book is the next step toward becoming an expert Arduinian. You'll build 70 complex and practical projects with this versatile microcontroller platform and gain advanced skills to design reliable, professional, user-friendly creations. You'll remote-control your Arduino via Bluetooth and instant messaging, improve the accuracy of clock projects with internet time servers, and automatically turn your Arduino off when it completes a task. You'll safely control AC mains power and higher currents and conserve battery with low-power and sleep modes. You'll also use Charlieplexing to control LED matrix displays, keep your Arduino running with a watchdog timer, communicate over longer wired distances with the RS232 and RS485 buses, and much more. Along the way, you'll build fun and useful devices like: • A camera-enabled circuit to stream videos • An MP3 player to listen to audio of your choice • A CAN bus circuit to gather speed and engine data from your car • A web server to display data captured with an ESP32 board • A PS/2 keyboard to improve your user interfaces and easily enter and display data Guided by an Arduino master, you'll harness dozens of sensors, motors, displays, and techniques to bring your own expert inventions to life. Requirements: Arduino Uno and other Arduino-compatible microcontrollers andUSBasp programmers. Some projects may require other inexpensive parts.

the hardware hacking handbook: The Hardware Hacker Andrew "bunnie" Huang, 2017-03-21 For over a decade, Andrew "bunnie" Huang, one of the world's most esteemed hackers, has shaped the fields of hacking and hardware, from his cult-classic book Hacking the Xbox to the open-source laptop Novena and his mentorship of various hardware startups and developers. In The Hardware Hacker, Huang shares his experiences in manufacturing and open hardware, creating an illuminating and compelling career retrospective. Huang's journey starts with his first visit to the staggering electronics markets in Shenzhen, with booths overflowing with capacitors, memory chips, voltmeters, and possibility. He shares how he navigated the overwhelming world of Chinese factories to bring chumby, Novena, and Chibitronics to life, covering everything from creating a Bill of Materials to choosing the factory to best fit his needs. Through this collection of personal essays and interviews on topics ranging from the legality of reverse engineering to a comparison of intellectual property practices between China and the United States, bunnie weaves engineering, law, and society into the tapestry of open hardware. With highly detailed passages on the ins and outs of manufacturing and a comprehensive take on the issues associated with open source hardware, The Hardware Hacker is an invaluable resource for aspiring hackers and makers.

the hardware hacking handbook: The Hardware Hacker Andrew Bunnie Huang, 2019-08-27 For over a decade, Andrew bunnie Huang, one of the world's most esteemed hackers, has shaped the fields of hacking and hardware, from his cult-classic book Hacking the Xbox to the open-source laptop Novena and his mentorship of various hardware startups and developers. In The Hardware Hacker, Huang shares his experiences in manufacturing and open hardware, creating an illuminating and compelling career retrospective. Huang's journey starts with his first visit to the staggering electronics markets in Shenzhen, with booths overflowing with capacitors, memory chips, voltmeters, and possibility. He shares how he navigated the overwhelming world of Chinese factories

to bring chumby, Novena, and Chibitronics to life, covering everything from creating a Bill of Materials to choosing the factory to best fit his needs. Through this collection of personal essays and interviews on topics ranging from the legality of reverse engineering to a comparison of intellectual property practices between China and the United States, bunnie weaves engineering, law, and society into the tapestry of open hardware. With highly detailed passages on the ins and outs of manufacturing and a comprehensive take on the issues associated with open source hardware, The Hardware Hacker is an invaluable resource for aspiring hackers and makers.

the hardware hacking handbook: Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn, Stephen Sims, 2018-04-05 Cutting-edge techniques for finding and fixing critical security flaws Fortify your network and avert digital catastrophe with proven strategies from a team of security experts. Completely updated and featuring 13 new chapters, Gray Hat Hacking, The Ethical Hacker’s Handbook, Fifth Edition explains the enemy’s current weapons, skills, and tactics and offers field-tested remedies, case studies, and ready-to-try testing labs. Find out how hackers gain access, overtake network devices, script and inject malicious code, and plunder Web applications and browsers. Android-based exploits, reverse engineering techniques, and cyber law are thoroughly covered in this state-of-the-art resource. And the new topic of exploiting the Internet of things is introduced in this edition. •Build and launch spoofing exploits with Ettercap •Induce error conditions and crash software using fuzzers •Use advanced reverse engineering to exploit Windows and Linux software •Bypass Windows Access Control and memory protection schemes •Exploit web applications with Padding Oracle Attacks •Learn the use-after-free technique used in recent zero days •Hijack web browsers with advanced XSS attacks •Understand ransomware and how it takes control of your desktop •Dissect Android malware with JEB and DAD decompilers •Find one-day vulnerabilities with binary diffing •Exploit wireless systems with Software Defined Radios (SDR) •Exploit Internet of things devices •Dissect and exploit embedded devices •Understand bug bounty programs •Deploy next-generation honeypots •Dissect ATM malware and analyze common ATM attacks •Learn the business side of ethical hacking

the hardware hacking handbook: A Complete Hacker's Handbook Dr. K., 2000 No area of computing has generated as much mythology, speculation and sheer fascination as hacking. From Hollywood's perception of hackers as sinister, threatening cyberwizards to the computer trades' claim that such people are nothing more than criminal nerds, misunderstandings abound.

the hardware hacking handbook: *Gray Hat Hacking The Ethical Hackers Handbook, 3rd Edition* Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams, 2011-02-05 THE LATEST STRATEGIES FOR UNCOVERING TODAY'S MOST DEVASTATING ATTACKS Thwart malicious network intrusion by using cutting-edge techniques for finding and fixing security flaws. Fully updated and expanded with nine new chapters, Gray Hat Hacking: The Ethical Hacker's Handbook, Third Edition details the most recent vulnerabilities and remedies along with legal disclosure methods. Learn from the experts how hackers target systems, defeat production schemes, write malicious code, and exploit flaws in Windows and Linux systems. Malware analysis, penetration testing, SCADA, VoIP, and Web security are also covered in this comprehensive resource. Develop and launch exploits using BackTrack and Metasploit Employ physical, social engineering, and insider attack techniques Build Perl, Python, and Ruby scripts that initiate stack buffer overflows Understand and prevent malicious content in Adobe, Office, and multimedia files Detect and block client-side, Web server, VoIP, and SCADA attacks Reverse engineer, fuzz, and decompile Windows and Linux software Develop SQL injection, cross-site scripting, and forgery exploits Trap malware and rootkits using honeypots and SandBoxes

the hardware hacking handbook: *There's No Such Thing as Crypto Crime* Nick Furneaux, 2024-10-30 Hands-on guidance for professionals investigating crimes that include cryptocurrency In There’s No Such Thing as Crypto Crime: An Investigators Guide, accomplished cybersecurity and forensics consultant Nick Furneaux delivers an expert discussion of the key methods used by cryptocurrency investigators, including investigations on Bitcoin and Ethereum type blockchains.

The book explores the criminal opportunities available to malicious actors in the crypto universe, as well as the investigative principles common to this realm. The author explains in detail a variety of essential topics, including how cryptocurrency is used in crime, exploiting wallets, and investigative methodologies for the primary chains, as well as digging into important areas such as tracing through contracts, coin-swaps, layer 2 chains and bridges. He also provides engaging and informative presentations of: Strategies used by investigators around the world to seize the fruits of crypto-related crime How non-fungible tokens, new alt-currency tokens, and decentralized finance factor into cryptocurrency crime The application of common investigative principles—like discovery—to the world of cryptocurrency An essential and effective playbook for combating crypto-related financial crime, There's No Such Thing as Crypto Crime will earn a place in the libraries of financial investigators, fraud and forensics professionals, and cybercrime specialists.

the hardware hacking handbook: Hardware Hacking Projects for Geeks Scott Fullam, 2004-01-28 A collection of unusual projects for computer hardware geeks of all ages explains how to create such projects as a personal Lojack system, Web-enabled coffee machine, cubicle intrusion detection systems, and a laptop battery extender.

the hardware hacking handbook: Hacking the Xbox Andrew Huang, 2003 This hands-on guide to hacking was canceled by the original publisher out of fear of DMCA-related lawsuits. Following the author's self-publication of the book (during which time he sold thousands directly), Hacking the Xbox is now brought to you by No Starch Press. Hacking the Xbox begins with a few step-by-step tutorials on hardware modifications that teach basic hacking techniques as well as essential reverse-engineering skills. It progresses into a discussion of the Xbox security mechanisms and other advanced hacking topics, emphasizing the important subjects of computer security and reverse engineering. The book includes numerous practical guides, such as where to get hacking gear, soldering techniques, debugging tips, and an Xbox hardware reference guide. Hacking the Xbox confronts the social and political issues facing today's hacker, and introduces readers to the humans behind the hacks through several interviews with master hackers. It looks at the potential impact of today's

the hardware hacking handbook: *Practical Hardware Pentesting* Jean-Georges Valle, 2021-04-01 Learn how to pentest your hardware with the most common attract techniques and patterns Key FeaturesExplore various pentesting tools and techniques to secure your hardware infrastructureProtect your hardware by finding potential entry points like glitchesFind the best practices for securely designing your productsBook Description If you're looking for hands-on introduction to pentesting that delivers, then Practical Hardware Pentesting is for you. This book will help you plan attacks, hack your embedded devices, and secure the hardware infrastructure. Throughout the book, you will see how a specific device works, explore the functional and security aspects, and learn how a system senses and communicates with the outside world. You'll set up a lab from scratch and then gradually work towards an advanced hardware lab—but you'll still be able to follow along with a basic setup. As you progress, you'll get to grips with the global architecture of an embedded system and sniff on-board traffic, learn how to identify and formalize threats to the embedded system, and understand its relationship with its ecosystem. You'll discover how to analyze your hardware and locate its possible system vulnerabilities before going on to explore firmware dumping, analysis, and exploitation. The reverse engineering chapter will get you thinking from an attacker point of view; you'll understand how devices are attacked, how they are compromised, and how you can harden a device against the most common hardware attack vectors. By the end of this book, you will be well-versed with security best practices and understand how they can be implemented to secure your hardware. What you will learnPerform an embedded system test and identify security critical functionalitiesLocate critical security components and buses and learn how to attack them Discover how to dump and modify stored informationUnderstand and exploit the relationship between the firmware and hardwareIdentify and attack the security functions supported by the functional blocks of the deviceDevelop an attack lab to support advanced device analysis and attacksWho this book is for If you're a researcher or a security professional who wants a

comprehensive introduction into hardware security assessment, then this book is for you. Electrical engineers who want to understand the vulnerabilities of their devices and design them with security in mind will also find this book useful. You won't need any prior knowledge with hardware pentensting before you get started; everything you need is in the chapters.

the hardware hacking handbook: Gray Hat Hacking, Second Edition Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, 2008-01-10 A fantastic book for anyone looking to learn the tools and techniques needed to break in and stay in. --Bruce Potter, Founder, The Shmoo Group Very highly recommended whether you are a seasoned professional or just starting out in the security business. --Simple Nomad, Hacker

the hardware hacking handbook: Hardware Hacker Andrew Huang, 2017

Related to the hardware hacking handbook

HWiNFO - Free System Information, Monitoring and Diagnostics Free Hardware Analysis, Monitoring and Reporting. In-depth Hardware Information, Real-Time System Monitoring, Reporting & more

Free Download HWiNFO Sofware | Installer & Portable for Start to analyze your hardware right now! HWiNFO has available as an Installer and Portable version for Windows (32/64-bit) and Portable version for DOS

About HWiNFO Software - Professional System Information Comprehensive Hardware Information Exhaustive information about hardware components displayed in hierarchy unfolding into deep details. Useful for obtaining a detailed hardware

[SOLVED] - I don't have an option to enable hardware acceleration I'm using windows 10 PRO 1909 , build 18363 and I couldn't find the option in the display settings. I also couldn't find anything in the Nvidia Control Panel. Any help on the topic

[SOLVED] - LiveKernelEvent error | Tom's Hardware Forum Hi, so every now and then my pc crashes. My screen turns off and my keyboard and mouse stop working. The only way I can turn off my pc after this happens is by manually

Add-ons | HWiNFO A Windows console application designed to present various hardware sensor parameters reported by HWiNFO® as a JSON string and make it available over the network

[SOLVED] - WHEA-Logger Event 19 - Tom's Hardware Forum What hardware in the pc? Have latest drivers? Latest windows updates? Latest bios?

[SOLVED] - Tom's Hardware Forum I had to unplug my computer equipment for a couple of days. When I connected it all back up again my MX Master mouse was no longer working (with Windows 10). I tried

[SOLVED] - Unable to activate Windows after - Tom's Hardware Select I changed hardware on this device recently, then select Next. Enter your connected Microsoft account and password, then select Sign in. The troubleshooter will only

Featured content - Tom's Hardware Forum Join the discussion about the latest in computer hardware, software, and gadgets in the Tom's Hardware Community! Catch everything from expert opinion to casual buzz in our

HWiNFO - Free System Information, Monitoring and Diagnostics Free Hardware Analysis, Monitoring and Reporting. In-depth Hardware Information, Real-Time System Monitoring, Reporting & more

Free Download HWiNFO Sofware | Installer & Portable for Windows, Start to analyze your hardware right now! HWiNFO has available as an Installer and Portable version for Windows (32/64-bit) and Portable version for DOS

About HWiNFO Software - Professional System Information Comprehensive Hardware Information Exhaustive information about hardware components displayed in hierarchy unfolding into deep details. Useful for obtaining a detailed hardware

[SOLVED] - I don't have an option to enable hardware acceleration I'm using windows 10 PRO 1909 , build 18363 and I couldn't find the option in the display settings. I also couldn't find

anything in the Nvidia Control Panel. Any help on the topic

[SOLVED] - LiveKernelEvent error | Tom's Hardware Forum Hi, so every now and then my pc crashes. My screen turns off and my keyboard and mouse stop working. The only way I can turn off my pc after this happens is by manually

Add-ons | HWiNFO A Windows console application designed to present various hardware sensor parameters reported by HWiNFO® as a JSON string and make it available over the network

[SOLVED] - WHEA-Logger Event 19 - Tom's Hardware Forum What hardware in the pc? Have latest drivers? Latest windows updates? Latest bios?

[SOLVED] - Tom's Hardware Forum I had to unplug my computer equipment for a couple of days. When I connected it all back up again my MX Master mouse was no longer working (with Windows 10). I tried

[SOLVED] - Unable to activate Windows after - Tom's Hardware Select I changed hardware on this device recently, then select Next. Enter your connected Microsoft account and password, then select Sign in. The troubleshooter will only

Featured content - Tom's Hardware Forum Join the discussion about the latest in computer hardware, software, and gadgets in the Tom's Hardware Community! Catch everything from expert opinion to casual buzz in our

HWiNFO - Free System Information, Monitoring and Diagnostics Free Hardware Analysis, Monitoring and Reporting. In-depth Hardware Information, Real-Time System Monitoring, Reporting & more

Free Download HWiNFO Sofware | Installer & Portable for Windows, Start to analyze your hardware right now! HWiNFO has available as an Installer and Portable version for Windows (32/64-bit) and Portable version for DOS

About HWiNFO Software - Professional System Information Comprehensive Hardware Information Exhaustive information about hardware components displayed in hierarchy unfolding into deep details. Useful for obtaining a detailed hardware

[SOLVED] - I don't have an option to enable hardware acceleration I'm using windows 10 PRO 1909 , build 18363 and I couldn't find the option in the display settings. I also couldn't find anything in the Nvidia Control Panel. Any help on the topic

[SOLVED] - LiveKernelEvent error | Tom's Hardware Forum Hi, so every now and then my pc crashes. My screen turns off and my keyboard and mouse stop working. The only way I can turn off my pc after this happens is by manually

Add-ons | HWiNFO A Windows console application designed to present various hardware sensor parameters reported by HWiNFO® as a JSON string and make it available over the network

[SOLVED] - WHEA-Logger Event 19 - Tom's Hardware Forum What hardware in the pc? Have latest drivers? Latest windows updates? Latest bios?

[SOLVED] - Tom's Hardware Forum I had to unplug my computer equipment for a couple of days. When I connected it all back up again my MX Master mouse was no longer working (with Windows 10). I tried

[SOLVED] - Unable to activate Windows after - Tom's Hardware Select I changed hardware on this device recently, then select Next. Enter your connected Microsoft account and password, then select Sign in. The troubleshooter will only

Featured content - Tom's Hardware Forum Join the discussion about the latest in computer hardware, software, and gadgets in the Tom's Hardware Community! Catch everything from expert opinion to casual buzz in our

HWiNFO - Free System Information, Monitoring and Diagnostics Free Hardware Analysis, Monitoring and Reporting. In-depth Hardware Information, Real-Time System Monitoring, Reporting & more

Free Download HWiNFO Sofware | Installer & Portable for Windows, Start to analyze your hardware right now! HWiNFO has available as an Installer and Portable version for Windows (32/64-bit) and Portable version for DOS

About HWiNFO Software - Professional System Information Comprehensive Hardware Information Exhaustive information about hardware components displayed in hierarchy unfolding into deep details. Useful for obtaining a detailed hardware

[SOLVED] - I don't have an option to enable hardware acceleration I'm using windows 10 PRO 1909 , build 18363 and I couldn't find the option in the display settings. I also couldn't find anything in the Nvidia Control Panel. Any help on the topic

[SOLVED] - LiveKernelEvent error | Tom's Hardware Forum Hi, so every now and then my pc crashes. My screen turns off and my keyboard and mouse stop working. The only way I can turn off my pc after this happens is by manually

Add-ons | HWiNFO A Windows console application designed to present various hardware sensor parameters reported by HWiNFO® as a JSON string and make it available over the network

[SOLVED] - WHEA-Logger Event 19 - Tom's Hardware Forum What hardware in the pc? Have latest drivers? Latest windows updates? Latest bios?

[SOLVED] - Tom's Hardware Forum I had to unplug my computer equipment for a couple of days. When I connected it all back up again my MX Master mouse was no longer working (with Windows 10). I tried

[SOLVED] - Unable to activate Windows after - Tom's Hardware Select I changed hardware on this device recently, then select Next. Enter your connected Microsoft account and password, then select Sign in. The troubleshooter will only

Featured content - Tom's Hardware Forum Join the discussion about the latest in computer hardware, software, and gadgets in the Tom's Hardware Community! Catch everything from expert opinion to casual buzz in our

HWiNFO - Free System Information, Monitoring and Diagnostics Free Hardware Analysis, Monitoring and Reporting. In-depth Hardware Information, Real-Time System Monitoring, Reporting & more

Free Download HWiNFO Sofware | Installer & Portable for Start to analyze your hardware right now! HWiNFO has available as an Installer and Portable version for Windows (32/64-bit) and Portable version for DOS

About HWiNFO Software - Professional System Information Comprehensive Hardware Information Exhaustive information about hardware components displayed in hierarchy unfolding into deep details. Useful for obtaining a detailed hardware

[SOLVED] - I don't have an option to enable hardware acceleration I'm using windows 10 PRO 1909 , build 18363 and I couldn't find the option in the display settings. I also couldn't find anything in the Nvidia Control Panel. Any help on the topic

[SOLVED] - LiveKernelEvent error | Tom's Hardware Forum Hi, so every now and then my pc crashes. My screen turns off and my keyboard and mouse stop working. The only way I can turn off my pc after this happens is by manually

Add-ons | HWiNFO A Windows console application designed to present various hardware sensor parameters reported by HWiNFO® as a JSON string and make it available over the network

[SOLVED] - WHEA-Logger Event 19 - Tom's Hardware Forum What hardware in the pc? Have latest drivers? Latest windows updates? Latest bios?

[SOLVED] - Tom's Hardware Forum I had to unplug my computer equipment for a couple of days. When I connected it all back up again my MX Master mouse was no longer working (with Windows 10). I tried

[SOLVED] - Unable to activate Windows after - Tom's Hardware Select I changed hardware on this device recently, then select Next. Enter your connected Microsoft account and password, then select Sign in. The troubleshooter will only

Featured content - Tom's Hardware Forum Join the discussion about the latest in computer hardware, software, and gadgets in the Tom's Hardware Community! Catch everything from expert opinion to casual buzz in our

HWiNFO - Free System Information, Monitoring and Diagnostics Free Hardware Analysis,

Monitoring and Reporting. In-depth Hardware Information, Real-Time System Monitoring, Reporting & more

Free Download HWiNFO Sofware | Installer & Portable for Windows, Start to analyze your hardware right now! HWiNFO has available as an Installer and Portable version for Windows (32/64-bit) and Portable version for DOS

About HWiNFO Software - Professional System Information Comprehensive Hardware Information Exhaustive information about hardware components displayed in hierarchy unfolding into deep details. Useful for obtaining a detailed hardware

[SOLVED] - I don't have an option to enable hardware acceleration I'm using windows 10 PRO 1909 , build 18363 and I couldn't find the option in the display settings. I also couldn't find anything in the Nvidia Control Panel. Any help on the topic

[SOLVED] - LiveKernelEvent error | Tom's Hardware Forum Hi, so every now and then my pc crashes. My screen turns off and my keyboard and mouse stop working. The only way I can turn off my pc after this happens is by manually

Add-ons | HWiNFO A Windows console application designed to present various hardware sensor parameters reported by HWiNFO® as a JSON string and make it available over the network

[SOLVED] - WHEA-Logger Event 19 - Tom's Hardware Forum What hardware in the pc? Have latest drivers? Latest windows updates? Latest bios?

[SOLVED] - Tom's Hardware Forum I had to unplug my computer equipment for a couple of days. When I connected it all back up again my MX Master mouse was no longer working (with Windows 10). I tried

[SOLVED] - Unable to activate Windows after - Tom's Hardware Select I changed hardware on this device recently, then select Next. Enter your connected Microsoft account and password, then select Sign in. The troubleshooter will only

Featured content - Tom's Hardware Forum Join the discussion about the latest in computer hardware, software, and gadgets in the Tom's Hardware Community! Catch everything from expert opinion to casual buzz in our

Related to the hardware hacking handbook

JTAG Hacking An SSD With A Pi: A Primer (Hackaday1y) [Matthew “wrongbaud” Alt] is well known around these parts for his hardware hacking and reverse-engineering lessons, and today he’s bringing us a JTAG hacking primer that demoes some cool new hardware

JTAG Hacking An SSD With A Pi: A Primer (Hackaday1y) [Matthew “wrongbaud” Alt] is well known around these parts for his hardware hacking and reverse-engineering lessons, and today he’s bringing us a JTAG hacking primer that demoes some cool new hardware

A $500 Open Source Tool Lets Anyone Hack Computer Chips With Lasers (Wired1y) In modern microchips, where some transistors have been shrunk to less than a 10th of the size of a Covid-19 virus, it doesn't take much to mess with the minuscule electrical charges that serve as the

A $500 Open Source Tool Lets Anyone Hack Computer Chips With Lasers (Wired1y) In modern microchips, where some transistors have been shrunk to less than a 10th of the size of a Covid-19 virus, it doesn't take much to mess with the minuscule electrical charges that serve as the

Trump campaign turns to secure hardware after hacking incident (Reuters11mon) Oct 11 (Reuters) - Republican presidential candidate Donald Trump’s campaign is now using specialized, encrypted mobile phones and secure laptops in an effort to protect staff following a series of

Trump campaign turns to secure hardware after hacking incident (Reuters11mon) Oct 11 (Reuters) - Republican presidential candidate Donald Trump’s campaign is now using specialized, encrypted mobile phones and secure laptops in an effort to protect staff following a series of

Back to Home: http://142.93.153.27