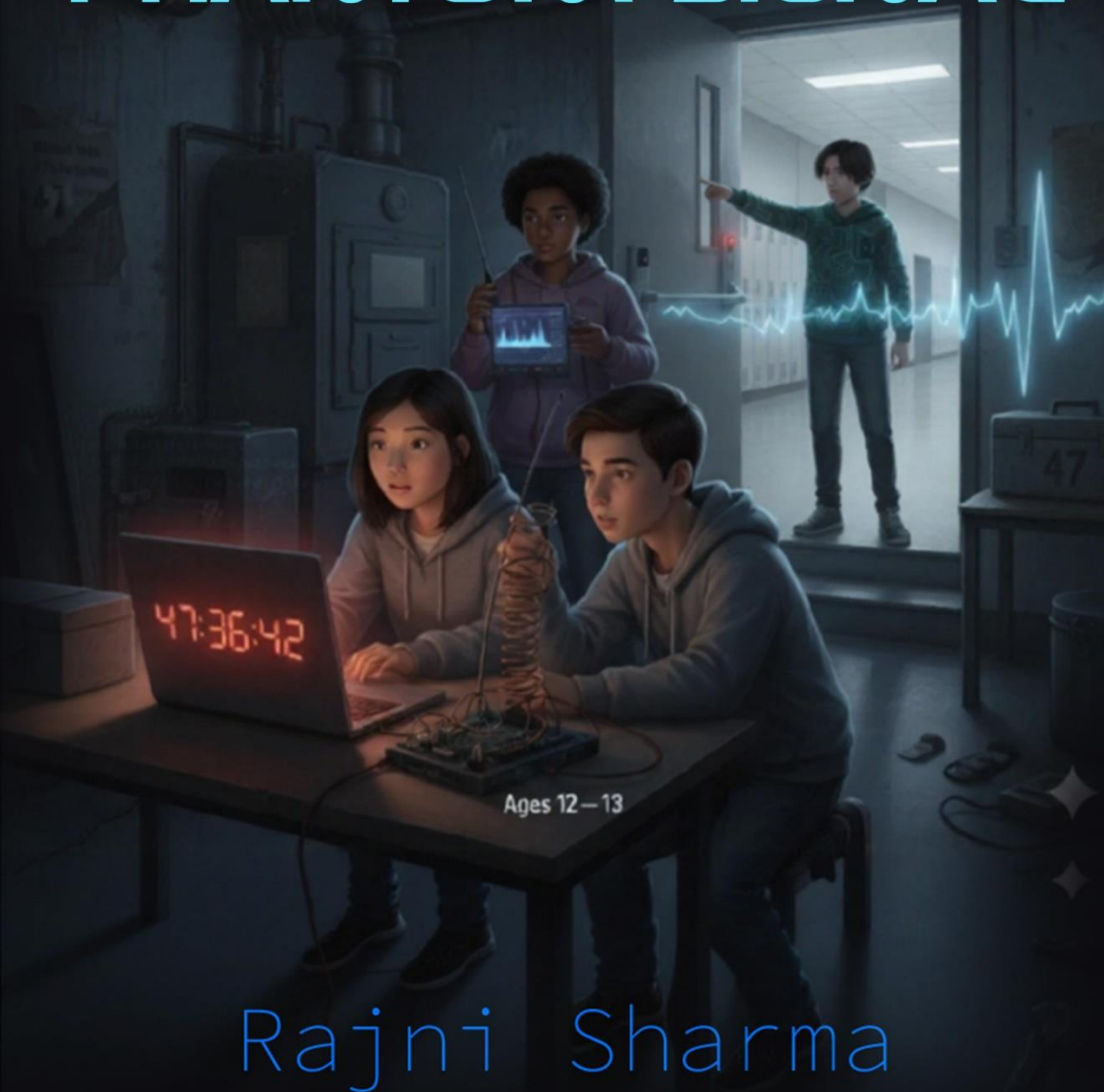


THE CYPHER KIDS & THE PHANTOM SIGNAL





The Cypher Kids and the Phantom Signal

A Hardware Hacking Adventure

Ages 12-13



<https://pagenest.in/>

Copyright

© 2025 Rajni Sharma

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the prior written permission of the publisher.

This book is intended for educational and entertainment purposes. While every effort has been made to ensure accuracy, the author and publisher are not responsible for any errors or omissions. All characters and scenarios are fictional and created to support learning in a fun and engaging way.

Important Disclaimer

The actions taken by the Cypher Kids, such as scanning the school network without permission, are fictional and shown with consequences to teach ethical lessons. In real life, such actions may violate school policies or laws, even if done with good intentions. Always obtain explicit permission before accessing or testing any system you don't own. The activities in this appendix are safe, legal, and designed for learning with parent or guardian approval.

The Series

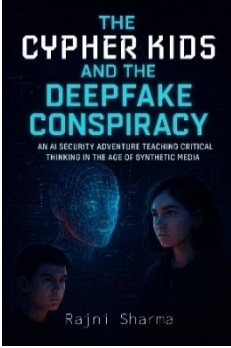
	Book 1: The Cypher Kids and the Glitch That Stole the Game Join Maya, Leo, and Sania as they dive into their first real cybersecurity mystery—tracking a hacker who’s sabotaging their school’s tech fair. Along the way, readers learn real coding and cyber safety skills through a thrilling adventure about teamwork, ethics, and digital responsibility.
	Book 2: The Cypher Kids and the Phantom Signal When strange radio signals threaten to lock down their smart school, the Cypher Kids must uncover a high-tech hardware conspiracy. This fast-paced story blends mystery, maker culture, and real-world lessons about IoT security, showing how curiosity and integrity can outsmart danger.
	Book 3: The Cypher Kids and the Deepfake Conspiracy A viral video sparks chaos—and only the Cypher Kids can prove it’s fake before their school’s reputation is destroyed. This gripping AI mystery teaches readers to question what they see online, revealing how critical thinking and truth can fight misinformation in the digital age.

Table of Contents

PROLOGUE: 48 HOURS UNTIL LOCKDOWN.....	1
CHAPTER 1: THE SMART SCHOOL INITIATIVE.....	5
CHAPTER 2: THE WIRELESS LANDSCAPE.....	18
CHAPTER 3: HARDWARE FORENSICS.....	28
CHAPTER 4: THE SUPPLY CHAIN ATTACK.....	42
CHAPTER 5: BUILDING THE DETECTOR.....	60
CHAPTER 6: THE SIGNAL MAP	77
CHAPTER 7: THE COUNTER-SIGNAL.....	89
CHAPTER 8: THE INFILTRATION PLAN.....	107
CHAPTER 9: THE PHYSICAL PENETRATION TEST...	131
CHAPTER 10: THE SIGNAL JAMMING.....	151
CHAPTER 11: THE TRIGGER TIME	174
CHAPTER 12: TRACKING THE SOURCE	193
CHAPTER 13: THE TAKEDOWN.....	216
CHAPTER 14: THE NEW HARDWARE LAB	233
EPILOGUE: THE NEXT SIGNAL.....	243
APPENDIX: HARDWARE SECURITY & IoT INVESTIGATION.....	253

PROLOGUE: 48 HOURS UNTIL LOCKDOWN

[Thursday, September 25, 11:23 PM]

The basement of Lincoln Middle School wasn't supposed to be this cold.

Maya Chen's breath came out in small clouds as she stared at the laptop screen, her fingers trembling—though not from the temperature. The numbers glowed an ominous red:

47:36:42

Forty-seven hours. Thirty-six minutes. Forty-two seconds until Saturday, September 27 at noon. And counting down.

"Tell me I'm wrong," she whispered, though she knew she wasn't. She'd checked the signal patterns seventeen times. Seventeen times, the same result.

Leo Rodriguez crouched beside the Raspberry Pi they'd hidden behind the old boiler three days ago. Its antenna—a homemade wire job that looked like it belonged in a spy movie—pointed toward the ceiling. Toward the new wing. Toward every smart lock installed six months ago.

"You're not wrong." Leo's voice was flat. Dead. "If this frequency hits at the timestamp in the code..."

He didn't finish. He didn't need to.

Sania Okonjo held the radio scanner, watching the waterfall display of frequencies. Most were normal—WiFi routers, Bluetooth devices, cell phone chatter.

But there, at 433.92 MHz, a spike appeared.

Two seconds long.

Then gone.

The phantom signal. The one they'd been chasing for three weeks.

"It's broadcasting again," Sania said, her voice tight. She pulled her hoodie closer. "Same pattern. Same frequency. It's like it's... testing. Making sure everything's ready."

Maya's screen flickered. New data scrolled past—packet captures from the school's network, pulled from monitoring tools they'd quietly installed after the mascot vote incident three months ago.

All of it pointed to one impossible, terrifying conclusion.

"Forty-seven doors," Maya said quietly, looking at the building schematics on her screen. "Every entrance. Every exit. Every classroom in the new wing." Her finger traced invisible patterns. "When this signal triggers, they all lock. Simultaneously."

"Students trapped inside during the weekend," Leo finished, his hacker instincts firing. "No way out. And the override codes won't work because the hardware doesn't match the software anymore."

The scanner beeped again. Another pulse. But this time, it was longer. Five seconds instead of two.

Sania's hands shook as she adjusted the settings. "That's not the test signal. That's—"

"Communication," Leo interrupted. "Someone just sent a command. Or received one."

They exchanged glances in the dim emergency lighting.

"We have to tell someone," Sania said, but her voice lacked conviction. After the mascot vote investigation, they'd learned that adults didn't always listen to students—even when the students were right.

"Mr. Peterson," Maya decided. "First thing tomorrow. We show him everything—the signal captures, the countdown, the hardware backdoors we found. All of it."

"What if he says we need to wait for proper authorization?" Leo asked. "What if he wants to go through channels?"

"Then we have forty-seven hours to convince him we don't have time for channels," Maya said firmly.

The scanner beeped again. Stronger this time.

And somewhere in the building above them, something clicked.

A door? A lock? A countdown initiating?

Leo grabbed his backpack. "We need to document everything. Right now. Photos, logs, evidence. If this goes sideways—"

"It won't," Maya said, though her voice wavered. "We solved the mascot vote attack. We can solve this too."

"That was software," Sania pointed out. "This is hardware. Physical backdoors installed in our building by someone with access."

"By someone professional," Leo added, staring at the signal patterns. "Look at the precision. The timing. The encryption. This isn't some student prank."

They all knew what that meant. The mascot vote investigation last spring—back in March and April—had taught them to distinguish between student mischief and professional attacks. That investigation had ended just as summer break started, with Alex serving his suspension. Now it was September, a new school year, and they were facing something even more sophisticated. Maya pulled out her investigation notebook—the fourth one since they'd started the Security Club after the mascot incident. She wrote:

OPERATION: PHANTOM SIGNAL Day 1 of investigation: 47 hours until unknown event Known: Countdown timer embedded in door controller firmware Known: 433.92 MHz signal broadcasts every 47 minutes Known: Someone installed hardware backdoors in 47 smart locks Unknown: Who, why, and what happens when timer hits zero

The emergency lights flickered.

In the darkness, the countdown glowed:

47:32:41

Three kids in a basement, staring at a screen, realizing that whoever had built this trap...

...knew they were trying to disarm it.

The phantom signal pulsed once more. And in that pulse, Maya could have sworn she heard a pattern. A rhythm.

Four-seven. Four-seven. Four-seven.

That number again. It meant something. It had to.

But what?

"Monday morning," Maya said, closing her laptop. "We take everything to Mr. Peterson. Every signal capture, every log entry, every piece of evidence. He believed us about the mascot vote. He'll believe us now."

"And if the countdown is real?" Sania asked quietly. "If something actually happens in forty-seven hours?"

Maya looked at her friends—her team. The Cypher Kids. They'd investigated a sophisticated voting attack together three months ago. They'd learned to document everything, think critically, and work within proper boundaries.

They could do this.

They had to.

"Then we make sure we're ready," Maya said. "Together."

"Together," Leo and Sania echoed.

But as they climbed the basement stairs, none of them saw the small red light that blinked to life on the Raspberry Pi.

Someone was watching their monitoring equipment.

Someone knew they'd found the countdown.

And someone was adjusting their plans accordingly.

CHAPTER 1: THE SMART SCHOOL INITIATIVE

[Monday, September 8 - Three Weeks Before the Countdown]

Maya Chen was the first to notice the door.

Not because she was looking for it—she was actually trying to avoid being late to homeroom after a long weekend—but because it *hissed* when it opened.

That wasn't right.

Lincoln Middle School's doors had always creaked. They'd groaned and squeaked and occasionally refused to close properly. But they'd never hissed. Never made that smooth, pneumatic *whoosh* of something electronic and expensive.

She stopped, staring at the door to Mrs. Patterson's classroom as it swung shut with mechanical precision. A small keypad glowed beside the frame. Green LED. New hardware smell. A tiny logo etched into the brushed aluminum: **SecureTech Solutions**.

Maya pulled out her phone and took a photo. Old habits from the mascot vote investigation three months ago—document everything, Mr. Peterson always said.

"Cool, right?"

She jumped slightly. Leo Rodriguez appeared beside her, backpack slung over one shoulder, grinning.

"The smart lock thing?" he continued, gesturing at the keypad. "They installed them over summer break. Whole building. My mom works in the district office—she says it cost two million dollars."

Two million dollars. For door locks.

Maya's brain—always calculating—did the math automatically. Lincoln MS had 147 doors (she'd counted during last year's fire drill). Two million divided by 147...

"That's over thirteen thousand dollars per door," she said aloud.

Leo shrugged. "Twenty-first century learning environment. Everything's smart now. Lights, thermostats, cameras. Apparently we're a pilot program for the whole district."

"Pilot program," Maya repeated slowly, her investigation instincts tingling. After the mascot vote incident—after discovering Mr. Martinez had covered up a data breach—she'd learned to be suspicious of new technology rolled out quickly.

The bell rang—electronic now, not the old mechanical buzz—and Maya hurried into homeroom.

She forgot about the doors for exactly four periods.

[12:23 PM - Cafeteria]

Maya spotted Sania Okonjo at their usual table and made her way through the lunch crowd. Since the mascot vote investigation and the formation of Security Club, the three of them—Maya, Leo, and Sania—had become inseparable.

"Did you notice the new door locks?" Maya asked, sliding into her seat.

Sania looked up from her phone, that focused expression Maya had learned to recognize. Something was bothering her.

"Yes. And I noticed something else." Sania turned her phone around. "Grace Liu just posted this in the class group chat."

The screenshot showed a notification:

[Smart Lock Alert - 08:31:47] Classroom 214 - Door Status: UNLOCKED Override Code: NONE Source: Unknown

"That's Mrs. Patterson's room," Maya said. "Grace is in her first period class."

"According to Grace, the door locked them out for ten minutes this morning," Sania said. "Mrs. Patterson had to call the office. They said it was a system glitch."

Maya felt that familiar pull—the beginning of a pattern, the edge of a mystery. "Just like the voting notifications last spring. Remember? Everyone dismissed those as glitches too."

"Until we proved they weren't," Leo said, dropping his lunch tray onto the table with a clatter. "Please tell me we're not investigating another school system hack. I was really looking forward to a normal year."

"Define normal," Sania said dryly. "We run Security Club now. We teach other students about cybersecurity. Normal left the building."

Security Club—which they'd founded in late May after the mascot vote investigation concluded—had grown from three founding members to fifteen regular attendees."

Leo pulled out his laptop—the same battered ThinkPad covered in Python stickers. "Fine. Let me see what I can find out about these smart locks."

He navigated to the school's public-facing IT dashboard—a system they'd learned about during the last investigation. The security was still surprisingly lax.

"There," Leo said, pointing at the screen. "IoT device management portal. And look—no authentication required for basic information."

The dashboard displayed:

LINCOLN MS - IoT DEVICE INVENTORY

- Smart Locks: 147 devices
- Smart Thermostats: 34 devices
- Security Cameras: 89 devices
- Total Connected Devices: 270

"Two hundred seventy Internet-connected devices," Maya breathed. "That's... a lot of attack surface."

"And look at this," Leo said, clicking through to the device details. "Vendor information. All the smart locks are from the same company: SecureTech Solutions."

Maya pulled out her investigation notebook—number four now, with "THE CYPHER KIDS" written on the cover in her neat handwriting. She flipped to a fresh page.

"SecureTech Solutions," she wrote. "Same company whose logo I saw on the door this morning."

"Let me search them," Sania said, already typing on her phone. After the mascot vote case, she'd become expert at OSINT—Open Source Intelligence. "Website looks professional. Founded two years ago. Specializes in educational facility security..."

She trailed off, scrolling.

"What?" Maya asked.

"They have contracts with thirty-eight schools across four states," Sania said slowly. "All installed in the last eighteen months. And look at the client testimonials—they're all five stars, but they read like they were written by AI."

Leo was examining the technical specifications. "These locks run on something called GlitchAPI. That name sounds familiar..."

His eyes widened. "Oh no. Maya, remember when Alex showed us his GitHub repositories? The abandoned framework with all the security vulnerabilities?"

Maya felt her stomach drop. "GlitchAPI version 0.3. The one with SQL injection vulnerabilities, no rate limiting, default credentials never changed..."

"The one the developer abandoned two years ago with a note saying 'please don't use this in production,'" Leo finished. "Our school just installed 147 door locks running on it."

The three of them stared at each other.

"We need to tell Mr. Peterson," Sania said. "Right now."

"And say what?" Leo asked. "We think the new security system might be insecure based on... what? A framework name and some AI-written testimonials?"

"Based on our experience," Maya said firmly. "We investigated a major security breach three months ago. We have credibility now. Mr. Peterson will listen."

"Will he?" Sania asked quietly. "Or will he tell us we're being paranoid? That we're seeing threats where there aren't any?"

Maya thought about that. After the mascot vote investigation, they'd learned that adults didn't always take student concerns seriously—even when those students were right. Even after they'd been proven right once before.

"We need more evidence," she decided. "Solid, undeniable proof that there's actually a problem. Not just 'this framework is old' or 'the testimonials look fake.' Real evidence."

"Like what?" Leo asked.

"Like the event logs," Maya said. "If Mrs. Patterson's door unlocked itself at 8:31 this morning, that should be in the system logs. We check the logs, see if there are other anomalous events, build a pattern."

"And if there is a pattern?" Sania asked.

"Then we document it completely and take it to Mr. Peterson," Maya said. "Just like we did with the voting manipulation. Thorough investigation, clear evidence, proper escalation."

She opened her notebook and wrote:

INVESTIGATION: SMART LOCK ANOMALIES

Day 1 - Observations:

- All doors replaced with "smart locks" over summer
- Vendor: SecureTech Solutions
- 147 locks installed (~\$2M total cost)
- Morning incident: Room 214 unlocked at 8:31:47 AM without authorization

- Technical concern: Locks run on GlitchAPI v0.3 (known vulnerable framework)

Questions:

- How many other "anomalous events" have occurred?
- Who has access to the system?
- What are the default credentials?
- Has anyone changed them?
- Why was GlitchAPI chosen despite known vulnerabilities?

Next steps:

- Check system logs (if accessible)
- Research SecureTech Solutions more thoroughly
- Document any additional incidents
- Approach Mr. Peterson when we have complete picture

"We're really doing this again," Leo said, reading over her shoulder. "Another investigation."

"Better us than nobody," Sania said. "After what happened with Mr. Martinez covering up that data breach, we know the adults aren't always paying attention."

"Some adults," Maya corrected. "Mr. Peterson paid attention. Dr. Kowalski took action. Principal Rodriguez listened eventually."

"Eventually," Leo repeated. "After we had overwhelming evidence."

"Then we'll get overwhelming evidence," Maya said. "We know how to do this now. We document everything, we think critically, we work as a team, and we involve adults at the right time."

The lunch bell rang—that new electronic tone that Maya was starting to hate.

As they gathered their things, Sania's phone buzzed. She glanced at it and frowned.

"Another post in the group chat. Jordan Kim says his classroom door wouldn't lock during passing period. Teacher had to call maintenance."

"What room?" Maya asked.

"307. Third floor, new wing."

Maya added it to her notebook:

Incident 2: Room 307, door wouldn't lock, time unknown

"That's two incidents in one morning," Leo observed. "Could be coincidence. Could be a pattern forming."

"Or could be exactly what it looks like," Maya said. "A hastily installed system with security vulnerabilities starting to show problems."

"Or," Sania added quietly, "someone exploiting those vulnerabilities deliberately."

The three of them exchanged glances. After the mascot vote investigation—after discovering someone had been manipulating the voting system for weeks before they noticed—they knew that "glitches" weren't always accidents.

Sometimes they were attacks.

Sometimes they were warnings.

And sometimes, they were tests.

[3:30 PM - Security Club Meeting]

Room 142 had been their sanctuary since they'd founded Security Club three months ago. The walls were covered with posters about the OWASP Top 10, ethical hacking frameworks, and a memorial photo of Rocket—Alex's golden retriever who'd inspired the whole "guardian" philosophy they'd adopted.

Fifteen students showed up for the meeting—their biggest turnout yet. After word had spread about how they'd uncovered the data breach last spring, Security Club had become unexpectedly popular.

But today, Maya, Leo, and Sania arrived early to talk privately before the others arrived.

"I checked the public logs during study hall," Leo said, pulling up his laptop. "The school's IoT dashboard doesn't require authentication for viewing—only for making changes. Look at this."

He showed them a log file:

ANOMALOUS EVENTS - LAST 30 DAYS

```
[2025-09-15 03:47:23] Camera_Hallway_B2 - OFFLINE (2
minutes) [2025-09-16 23:18:45] Thermostat_Room_108 -
Temp changed 68°F → 85°F [2025-09-18 11:47:19]
Lock_Main_Entrance - UNLOCKED (no override) [2025-
09-19 02:34:56] Camera_Cafeteria_3 - OFFLINE (47
minutes) [2025-09-22 15:47:33] Lock_Room_214 -
UNLOCKED (no override) [2025-09-23 00:23:11]
Thermostat_Library - Temp changed 70°F → 55°F [2025-
09-25 03:47:18] Lock_Room_307 - ERROR: Failed to lock
```

...continuing with 34 more entries...

"Forty-one anomalous events in the last month," Leo said. "And look at the timestamps. A lot of them happen late at night or early morning—2 AM, 3 AM, times when no one's here to notice."

Maya leaned closer. "And look at this pattern. September 15th, 3:47 AM. September 19th, same time. September 25th, 3:47 AM again."

"The number 47," Sania breathed. "That's Alex's pattern. Rocket was born at 8:47 AM, so Alex always uses 47 in his timing."

"But Alex wouldn't be doing this," Leo said quickly. "He's interning with Dr. Kowalski now. He's doing legitimate security work. He wouldn't jeopardize that."

"I'm not saying it's Alex," Maya said. "I'm saying someone might be copying his pattern. Or..." she hesitated, "or it could be coincidence. We shouldn't jump to conclusions."

The door opened and Alex walked in, backpack over one shoulder. Since joining Security Club three months ago, he'd become a regular member—though there was still sometimes an awkward tension. He'd been the suspect they'd investigated, after all, even though he'd ultimately been trying to help.

"Hey," Alex said, spotting them huddled around Leo's laptop. "What's going on?"

Maya made a decision. They'd learned during the last investigation that excluding Alex had been a mistake. He'd been working alone, and that isolation had led him to make bad choices. Better to include him from the start.

"The new smart locks are showing anomalous behavior," she said. "We're seeing pattern of unauthorized unlocks, mostly happening overnight."

Alex set down his backpack and came over. His expression shifted immediately—from casual to focused. That same intense concentration he got when analyzing security problems.

"Show me the logs," he said.

Leo pulled them up. Alex scanned through them, his eyes moving quickly.

"GlitchAPI," he said after a moment. "I recognize the error message format. That's the framework I tried to warn Mr. Martinez about two years ago."

"The school's using it for the new locks," Sania confirmed.

Alex's jaw tightened. "Of course they are. Because why learn from past mistakes when you can repeat them with more expensive hardware?"

"We don't know if it's a security problem yet," Maya said carefully. "Could just be buggy software."

"Could be," Alex agreed. "Or could be someone exploiting known vulnerabilities. These timestamps—" he pointed at the screen, "—some of them look deliberate. The 3:47 pattern, the systematic testing of different locations, the escalation from cameras to thermostats to locks. That's reconnaissance."

"Reconnaissance for what?" Sania asked.

"For a bigger attack," Alex said grimly. "Someone's mapping out the system, testing what they can control, building up to something larger."

Maya pulled out her investigation notebook. "Okay. If this is reconnaissance, we need to understand who has the skills and access to do this. And we need to figure out their endgame before they execute it."

"And we need to do it carefully," Leo added, "with proper documentation and adult oversight. We're not going rogue like last time."

He glanced at Alex as he said it—not accusatory, but as a reminder. They'd all learned hard lessons about working within proper boundaries.

"Agreed," Alex said. "Everything documented, everything authorized. Dr. Kowalski taught me that legitimate security work requires transparency."

The door opened again, and more Security Club members filed in—students eager to learn about cybersecurity, inspired by the story of how the Cypher Kids had uncovered a real data breach.

Maya closed her notebook. "We continue this after the meeting," she said quietly. "For now, we teach tonight's lesson and act normal."

"What's the lesson?" Sania asked.

"IoT security basics," Maya said with a slight smile. "Seems relevant."

As the room filled with students, Maya couldn't shake the feeling that they were at the beginning of something bigger. The mascot vote investigation had been about software vulnerabilities. This felt different.

This felt physical. Tangible. Doors that could lock or unlock on command. Systems that controlled access to the entire building.

If someone was testing the smart locks, they weren't just playing around.

They were preparing.

For what, Maya didn't know yet.

But she intended to find out.

Before whatever was coming actually arrived.

[6:47 PM - Maya's Room]

That evening, Maya sat at her desk reviewing the day's findings. Her investigation notebook lay open, and she'd started building a timeline on her wall—index cards connected with string, just like she'd seen in detective shows.

Her phone buzzed. The Cypher Kids group chat—the private one, just the three of them:

Leo: *Those logs are bothering me. The 3:47 pattern appears 11 times in 30 days.*

Sania: *And always testing different systems. Cameras, thermostats, locks. Like someone's learning what they can control.*

Maya: *Alex said it looks like reconnaissance. What do we think?*

Leo: *I think we need to figure out who has access to the system. The logs show "no override" for the unauthorized unlocks. That means no one used an admin password.*

Sania: *So either someone hacked in remotely, or someone has physical access to the hardware.*

Maya: *Or both. Remember SecureTech installed these. They'd have physical access during installation.*

There was a pause in the chat. Then Leo typed:

Leo: *Are you thinking what I'm thinking?*

Maya: *That a security company might not be secure? That's literally what we learned last time.*

Sania: *We need to research SecureTech more thoroughly. OSINT deep dive. Find out who they really are.*

Maya: *Tomorrow. Let's each take a different angle. Leo, technical details and infrastructure. Sania, company background and people. I'll look at their other installations and see if other schools have had problems.*

Leo: *And Alex?*

Maya: *We keep him informed but let him focus on his internship. We don't want Dr. Kowalski thinking we're pulling him back into gray hat territory.*

Sania: *Agreed. He's finally doing things the right way. We protect that.*

Maya set down her phone and looked at her timeline wall. So far, she had:

ANOMALY TIMELINE:

- 41 events in 30 days
- Pattern: 11 events at X:47 timestamps
- Targets: Cameras, thermostats, locks
- No admin override used
- Escalating from surveillance → environmental control → physical access

She added a new card:

QUESTIONS:

- Who benefits from controlling building access?
- What happens if all doors lock/unlock simultaneously?

- Fire safety implications?
- Is this practice for something bigger?

Her mom called her for dinner, but Maya took one more photo of her timeline first. Document everything. That was the rule.

As she left her room, she didn't notice her computer screen flicker. Didn't see the brief spike in her network activity. Didn't know that someone, somewhere, was monitoring which students were asking questions about the smart lock system.

The reconnaissance wasn't just about the building's systems.

It was about identifying who might notice.

And Maya Chen had just painted a target on herself.

But she wouldn't realize that until it was almost too late.

CHAPTER 2: THE WIRELESS LANDSCAPE

[Tuesday, 3:15 PM - Before Security Club Meeting]

Maya arrived early to Room 142 to find Mr. Peterson talking with a student she recognized from hallway encounters—Jamie Park, a seventh-grader with a reputation for building weird electronics projects.

"Maya, perfect timing," Mr. Peterson said. "Jamie heard about Security Club through the morning announcements and is interested in joining. They have some relevant experience I thought you should hear about."

Jamie shifted their backpack—noticeably heavier than most students carried. "I, uh, do hardware stuff. Arduino, Raspberry Pi, that kind of thing. Built a weather station that tweets. And I've been getting into software-defined radio lately."

Maya's investigator instincts perked up. "SDR? That's for monitoring radio frequencies, right?"

"Yeah," Jamie said, warming up. "My dad got me one for my birthday. I've been listening to weather satellites and aircraft transponders. It's pretty cool seeing all the invisible signals around us."

"We're actually investigating some unusual behavior with the school's smart locks," Maya said, making a quick decision. "Would you be willing to help us understand the wireless side of things?"

"Definitely," Jamie said immediately.

Mr. Peterson smiled. "That's what I was hoping. Jamie, welcome to Security Club. You're joining at an interesting time."

[Tuesday, 3:47 PM - Security Club Meeting]

The next day's Security Club meeting had an unexpected addition.

"Everyone, this is Jamie Park," Mr. Peterson said, gesturing to a student Maya vaguely recognized from the hallways. "They're joining Security Club today. Jamie, want to tell everyone about yourself?"

Jamie stepped forward, a bit shy but clearly excited. They wore a hoodie with a circuit board pattern and carried a backpack that looked heavy with equipment.

"Hi. I'm Jamie. I'm really into hardware stuff—Raspberry Pi projects, Arduino, that kind of thing. I built a weather station last year that tweets temperature data every hour." They pulled out their phone to show photos. "And I've been getting into amateur radio lately. My dad got me an SDR—software-defined radio—for my birthday."

Maya's interest immediately sparked. "SDR? That's for listening to radio frequencies, right?"

"Yeah," Jamie said, warming up. "You can scan all kinds of signals. FM radio, weather satellites, aircraft transponders. Even some IoT devices that use RF instead of WiFi."

Leo and Maya exchanged glances. RF—radio frequency. The smart locks had to communicate somehow.

"What frequency ranges can your SDR pick up?" Leo asked.

"Mine covers 24 MHz to 1766 MHz, though there are gaps—it can't receive the cellular bands in the middle. But it gets FM radio, aircraft, weather satellites, and the 433 MHz band we're interested in." Jamie said. "Covers most of the common bands. WiFi, Bluetooth, Zigbee, those cheap 433 MHz garage door openers—"

"Wait," Maya interrupted. "433 MHz? What uses that?"

"Lots of stuff," Jamie said. "Wireless doorbells, car key fobs, garage doors, cheap wireless sensors. It's an unlicensed frequency, so anyone can use it without special permits. But it's also super insecure—no encryption usually, easy to intercept."

Sania caught Maya's eye. They were all thinking the same thing.

"Jamie," Mr. Peterson said, "the Cypher Kids have been investigating some unusual behavior in the school's new smart lock system. Would you be willing to help them understand the wireless side of things?"

"Definitely," Jamie said immediately. "I've been curious about those locks since they installed them. Want me to bring my SDR equipment tomorrow?"

"Actually," Maya said, making a decision, "could you bring it today? After the meeting? We'd love to learn how it works."

"Sure," Jamie agreed. "I have it in my locker."

[4:45 PM - Behind the School, Near the Server Room]

After the regular Security Club meeting ended, the core group—Maya, Leo, Sania, and now Jamie—gathered in a relatively secluded spot behind the building. Alex had texted that he couldn't make it; Dr. Kowalski had him working on a project at the district office.

Jamie unpacked their equipment: a small USB dongle connected to a Raspberry Pi, with a telescoping antenna attached. The Pi's screen showed a waterfall display of radio signals.

"This is an RTL-SDR," Jamie explained. "Costs about thirty dollars. Originally designed for watching TV on computers, but hackers figured out you could use it to receive almost any radio signal. Plug it into a Raspberry Pi, run some software, and boom—you've got a powerful radio scanner."

They pulled up a program called GQRX. The screen filled with a colorful waterfall pattern—waves of color representing different radio signals at different frequencies.

"Each vertical line is a signal," Jamie explained. "The brighter the color, the stronger the signal. See this big chunk at 2.4 GHz? That's WiFi. And this one at 5 GHz is more WiFi—newer, faster standard."

"What are we looking for?" Sania asked.

"Anything unusual," Maya said. "The smart locks have to communicate somehow. They're not all hardwired—some of them are wireless. We need to know what frequency they use."

"Let me scan the common IoT frequencies," Jamie said, adjusting the settings. They started at 300 MHz and slowly scanned upward.

At 433.92 MHz, something appeared.

A brief pulse. Two seconds long. Then nothing.

"What was that?" Leo asked.

"Not sure," Jamie said, watching the waterfall display. "Could be anything. Garage door, wireless doorbell, car key fob. That frequency is like the wild west—everyone uses it."

They waited. Forty-seven minutes later, another pulse. Same frequency. Same duration.

Maya checked her watch. "4:47 PM. And the pulse was exactly 47 minutes after the last one."

"That's not a coincidence," Sania said. "That's the pattern from the logs. Events at X:47."

Jamie adjusted the antenna, pointing it toward different parts of the building. "Let me see if I can tell where it's coming from. Signal strength varies with direction."

They tested four different angles:

- **Pointed at parking lot:** Weak signal
- **Pointed at old wing:** Weak signal
- **Pointed at new wing:** Strong signal
- **Pointed at server room:** Strongest signal

"It's coming from inside the building," Jamie confirmed. "Either the new wing or the server room. That's where the signal is strongest."

"Can you record it?" Maya asked. "Save the actual signal data?"

"Absolutely," Jamie said, typing commands into the Raspberry Pi. "I'll set it up to automatically record any transmissions on 433.92 MHz. We'll have a complete log of every time this signal broadcasts."

Leo pulled out his laptop and opened the school's IoT dashboard. "Let me check if there are any events in the logs at 4:47 PM."

He scrolled through recent entries:

```
[2025-09-29 16:47:12] Lock_Room_305 - Status check
(normal) [2025-09-29 16:47:18] Lock_Main_Entrance -
Status check (normal)
[2025-09-29 16:47:24] Lock_Server_Room - Status check
(normal)
```

"Status checks," Leo said. "The system is pinging the locks to verify they're online. And it's happening right when we detected the RF signal."

"So the locks are using 433 MHz to communicate," Sania concluded. "Not WiFi. Not Zigbee. Just basic, cheap RF."

"That's actually pretty concerning," Jamie said. "433 MHz has no built-in security. Anyone with an SDR can intercept the signals. Anyone with a transmitter can send fake signals. It's like having a conversation by shouting across a field—everyone can hear you."

Maya was writing in her notebook:

WIRELESS DISCOVERY:

- Smart locks communicate via 433.92 MHz RF
- Signal pulses every 47 minutes (status checks)
- No encryption on this frequency band
- Signal strongest near server room and new wing
- Anyone with \$30 SDR dongle can intercept signals

"Can you decode the actual signal?" Leo asked Jamie. "See what data is being transmitted?"

"Maybe," Jamie said. "These signals are usually pretty simple. On-off keying, amplitude modulation, basic encoding. Let me try to capture a clean signal and analyze it."

They waited for the next pulse at 5:47 PM. Jamie's software recorded it, and they examined the waveform.

"It's encoded," Jamie said, zooming in on the data. "But not encrypted—that's different. Encoding just means turning data into signals. Encryption means scrambling it so only authorized people can read it."

They spent twenty minutes analyzing the signal pattern. Finally, Jamie pointed at the screen.

"Look. This part here—" they highlighted a section of the waveform, "—that's a device ID. Uniquely identifies which lock is being communicated with. And this part is the command. Probably something like 'report status' or 'lock' or 'unlock.'"

"So if someone recorded this signal," Maya said slowly, "they could replay it. Make a lock think it's receiving a legitimate command."

"Exactly," Jamie confirmed. "That's called a replay attack. Record the 'unlock' command, transmit it back later, door opens."

"Even without knowing how the signal is encoded," Leo added. "You don't need to understand the language if you just repeat exactly what you heard."

Sania looked worried. "That means anyone with basic radio equipment could unlock any door in the building. Just by recording and replaying signals."

"Or they could jam the signals," Jamie said. "Transmit noise on 433.92 MHz and prevent the locks from receiving legitimate commands. Doors wouldn't work at all."

"Or," Maya said grimly, "they could transmit fake commands. Tell all the locks to open at once. Or close at once. Or stop responding to keypads."

They fell silent, the implications sinking in.

"This is worse than the mascot vote thing," Leo said quietly. "That was just data. This is physical access to the entire building."

Maya checked her watch. "It's 6:02 PM. We need to document everything we've learned and brief Mr. Peterson first thing tomorrow morning."

"Should we tell Alex?" Sania asked.

"Not yet," Maya decided. "He's got enough on his plate with his internship. We bring this to Mr. Peterson first, see what he says, then loop Alex in if needed."

Jamie was packing up their equipment. "I can leave the Raspberry Pi running overnight, hidden behind the dumpster here. It'll automatically record every 433.92 MHz signal. By tomorrow morning, we'll have a complete log of all the transmissions."

"That's perfect," Maya said. "We'll have data to show Mr. Peterson. Not just theories—actual evidence."

As they walked back toward the parking lot, Maya noticed something. A white van in the far corner, near the service entrance. Logo on the side: SecureTech Solutions.

"Installation van?" Leo suggested.

"Maybe," Maya said. "Or maintenance. Or..." she pulled out her phone and took a photo, "something else."

The van's license plate was visible. She made a note to run it through the DMV database—wait, no. That would be unauthorized access. Better to just document that it was here.

They split up to head home. Maya walked with Sania.

"You're thinking about something," Sania said. It wasn't a question. She could always read Maya's mood.

"The 47-minute pattern," Maya said. "The 433 MHz frequency. The lack of encryption. It's all so... deliberate. Like someone chose the least secure option possible."

"Or someone didn't know better," Sania offered. "Maybe SecureTech just used cheap hardware because it's cheap."

"Maybe," Maya said. But her investigator instincts were screaming that it was more than that.

When she got home, Maya went straight to her room and added to her timeline wall:

NEW FINDINGS - DAY 2:

- Smart locks use 433.92 MHz RF (insecure frequency)
- No encryption, just encoding
- Signals can be intercepted, recorded, replayed
- Anyone with \$30 SDR can listen
- Anyone with basic transmitter can send fake commands
- Status checks every 47 minutes (there's that number again)
- SecureTech van spotted on campus

She stepped back and looked at the bigger picture forming. The vulnerable framework (GlitchAPI). The insecure RF frequency. The lack of encryption. The pattern of X:47 timing.

Either this was catastrophically bad design...

Or it was intentionally vulnerable.

And if it was intentional, that meant someone had planned to exploit it from the very beginning.

Her phone buzzed. Jamie had sent a photo to the group chat—the Raspberry Pi hidden behind the dumpster, antenna extended, ready to record all night.

Jamie: *Monitor is running. Will collect data until 7 AM tomorrow. Should have complete record of all 433 MHz traffic.*

Leo: *That's going to be a lot of data. Every car key fob, every garage door opener, everything.*

Jamie: *I set up filters. Only recording signals that match the smart lock pattern—specific pulse duration and encoding style. Should keep the data manageable.*

Maya: *Perfect. Tomorrow morning, 7:30 AM, we meet before school and review the overnight data. Then we brief Mr. Peterson at 8 AM.*

Sania: *Assuming the data shows what we think it shows.*

Maya: *It will. The pattern is too consistent to be random.*

But as Maya settled into bed that night, she couldn't shake an uncomfortable feeling. They'd just set up surveillance equipment on school property. They were monitoring RF signals, analyzing wireless communications, collecting data about the school's security systems.

Were they investigating... or were they crossing the same lines Alex had crossed?

No, she decided. They were documenting a security vulnerability with the intent to report it to proper authorities. That was different from exploiting it. Different from attacking it.

As long as they followed their own rules—document everything, involve adults at the right time, don't cross ethical boundaries—they'd be okay.

She pulled out her notebook one more time and wrote:

ETHICAL CHECK - DAY 2:

- Are we authorized? No, but monitoring public airwaves is legal
- Are we harming anyone? No, only listening, not transmitting
- Are we planning proper disclosure? Yes, briefing Mr. Peterson tomorrow

- *Are we documenting everything? Yes, every step*
- *Would we be comfortable explaining our actions? Yes*

She closed the notebook, satisfied that they were still on the right side of the line.

Tomorrow would bring more answers. The overnight RF data would either confirm their suspicions or prove they were being paranoid.

But Maya didn't think they were being paranoid.

She thought they were onto something big.

And she thought whoever had installed these vulnerable locks knew exactly what they were doing.
