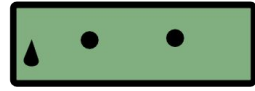


mithören

type, we'll listen

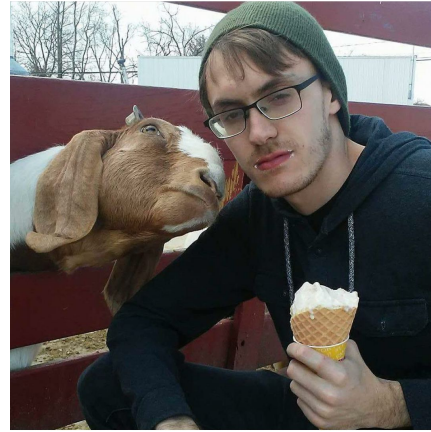


mithören

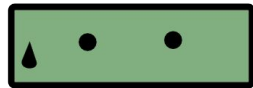
Intros



Colin Buckles



Michael Wolf

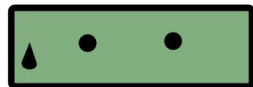


mithören

Problem Space

- Wireless technologies are inherently insecure
- Wireless keyboard vendors tend to value profit over security
- Dozens of exploits exist in the wild

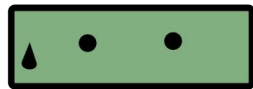




mithören

What Is Mithören?

- Mithören is a simple-to-use, extensible platform for wireless peripheral packet collection and interpretation
- We want to make keyboard security analysis available to all penetration testers and researchers



mithören

Our Solution

This one is done!



SAMY KAMKAR'S
KEYSWEEPER

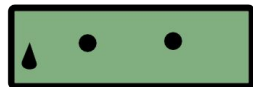



GNU Radio
the gnu software radio



Use Case





mithören

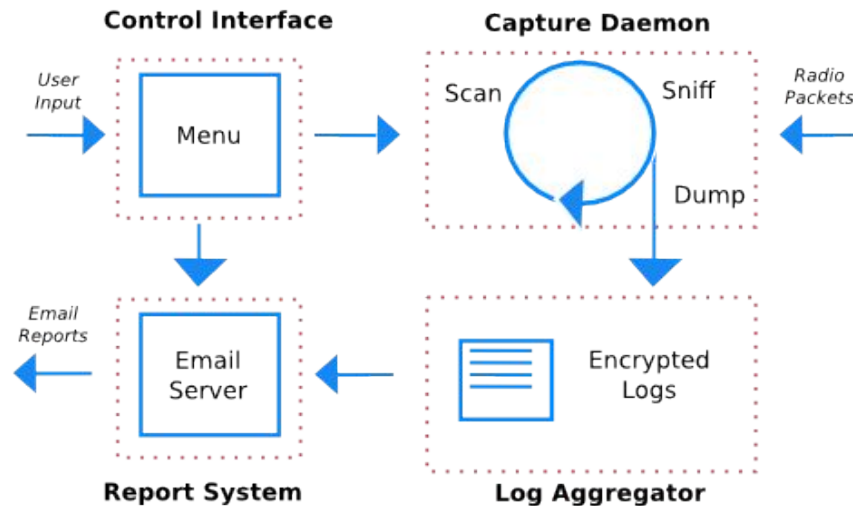
Architecture

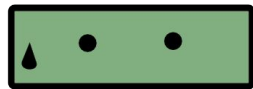
1. Daemon Process

- Sniffs airwaves
- Communicates with database

2. Control Interface

- Monitor process
- Configure process
- Send email





mithören

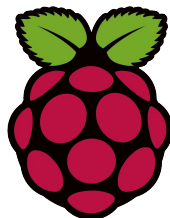
Tech Stack



POSTFIX



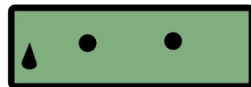
systemd



DOVECOT

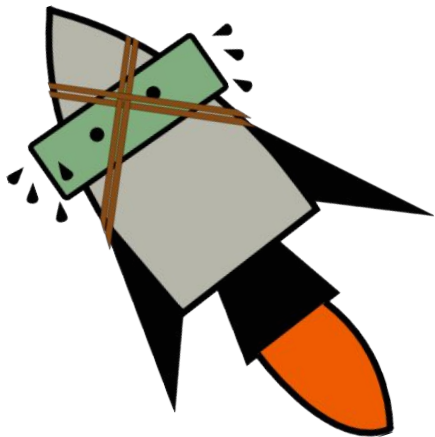
Demo

OwO

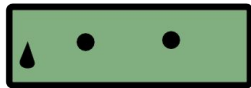


mithören

Next Steps



- PGP Encryption
- Additional modules
- Flesh-out device identification
- Integration into existing security tools
- Automated testing
- Security developer buy-in
- Get our email server out of spam filters

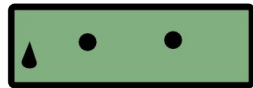


mithören

Thanks

-
- Bo Vyhovanyuk, Jim Scott
 - Bastille Research, Marc Newlin, Max Moser, Philipp Schrödel, fragil3,
 - Rohs Street Cafe, pilotredsun, AKIKO, Matthew Corbett
 - Richard Stallman

github.com/wolfmd/mith-ren



mithören

Conclusion

- Security-first manufacturing is vital to the defense of enterprises
- Consumer awareness = oversight
- Proactive testing with Mithören closes another gap in enterprise security

github.com/wolfmd/mith-ren

Questions?