HACKING HOTEL KEYS
And Point of Sale Systems

Security Consultant
TWITTER, LinkedIn @westonhecker
Rapid7 www.rapid7.com
“A Little Bit About Myself”

✓ Senior Security Engineer/Senior Pentester/ Security Researcher.


✓ 12 years programming and Reverse Engineering.

What Is This Talk About?

✓ Explain magstrip readers Magspoofeer. Difference from RFID
✓ Explain Modification to device.
✓ Hotel back ends explained, POS systems Explained
✓ Process of key checkout check in. Different parts of hotels.
✓ Attacks on Privileged Keys. Maids, Service, Fireman
✓ Encryption is just encoded.
What Is This Talk About?

- What lead to research on POS from hotel keys.
- How Do POS systems use magstripe readers.
- Trigger events and when the Reader listening and what is it listening for.
- Management cards on POS/card readers on the screen.
- How is a magstripe reader Used as a HID keyboard?.
- Injecting 102-US and proprietary keyboard layouts into binary data.
- Cash tend/Check tend attack.
- Attacking OS SQL injection CMD Drive by attack
- Restaurant attacks/other mag readers/Rewards programs and players cards on slot machines
Thanks to Samy Kamkar for his work.

• What is Magspoofer
How does a Magstripe Reader work
How magspoofer works what is SMT

- Explanation of Magspoofer+ and EM fields and how they interact with Heads on magnetic head reader this is not RFID Cards!!!
How To Handle Over Heating

100s of Cards = Heat
Explanation of PMS
Explanation of proprietary card readers and security behind hotel keys.
Collecting information from keys and reissued keys.
Interactions with different readers your door vs elevator external access and pool access.
Privileged cards Management, Maids, Service, Fireman law enforcement.
Examples of card Dumps Raw data from track 3 other tracks restaurant and Resort functions.

There are limitations on characters you can enter
Breaking the complex encryption of hotel keys... o it's simple encoding never mind.
Checking into your own hotel room
KIOSK research.
Point of Sale Systems

• What lead to this research after
  • hotel keys?
How do POS systems use magstripe readers?
Trigger events and when the Reader listening and what is it listening for.
• Management cards on
• POS/card readers on the screen.
How is a magstripe reader Used as a HID keyboard?
Injecting 102-US and proprietary keyboard layouts into binary data.
Cash tend/Check tend attack.
Behind every strong man is a strong woman and behind every POS there is an outdated OS.
Exiting POS Software.
Popping CMD downloading payload.
Payload overview what the bad guys would load.
Locked down and custom Dev'ed environments.
Limitations of mag injection/making a physical card attack/ limitations of physical can you make a waiter do your dirty work?
These devices are everywhere.
Injecting player rewards cards into Slot machines people already intentionally leave cards in machines for this purpose.
Rewards card point collecting rolling 10 different accounts/ Grocery store and gas stations
Injecting into prepaid/phone card activation/ activate at terminal swapping systems at POS
Trigger injection attacks "Sniffing USB reader" power up when power up is detected it triggers the EM read. Some companies ask to confirm account if only you could hit the enter key some how!!
Clock-In systems never be late for work again.
Going over 2 Demos

• Going to inject the Cash Tender

• And next I'm going to Install Credit Card Skimming Software with a Spoofer.
THANKS FOR COMING
Stay Legal

Security Consultant
TWITTER, LinkedIn @westonhecker
Rapid7 www.rapid7.com