TextSecure:
Encrypting phone calls / messages

“I've been telling you your whole life, don't talk on the phone. Now you understand huh?”
Goodfellas

Freddy Martinez
Cryptoparty Chicago

Reminder


Morgan Mayhem
@headhntr
Follow
"All phones are tapped. All strangers are the police." -- @attackerman #EncryptNews #OpSec
RETWEETS
45
FAVORITES
22
11:31 AM - 7 Nov 2014

Phones are not secure

A note about cell phones. Their principal function is location tracking. All other "features" are dependent on function

Never forget this fact

Seriously

Why do you need to encrypt?

- MetaData Leaks (SMS)
  - Carrier Choice
  - Language
- Lack of Forward Secrecy (Ki)
- GSM is so badly broken
- SMS spoofing attacks
- Cryptanalysis
  - DRTbox
  - Rainbox Tables (Schneider 2008) A5/1

Surveillance Capabilities

NSA

- Ki Theft
- WOLFMARITE

FBI / LEOs

- CellBrite
- IMSI Catcher
- DRTBox

Google

- HangOuts

Apple

- iMessage Key Escrow or signed RAMdisk ?

Smartphone Store

- TextSecure
  - Encrypted Text Messages
- Redphone (Android)
  - Encrypted Phone Calls
- Signal 2.0 (iOS 8)
  - Encrypted Phone and Text

How Does 'It' Work?

- Data channel between you and your recipient
- Generate encryption keys for *asynchronous* delivery
- Encrypted Database for message storing
- Every next message is encrypted with a new encryption key (PFS)

Axolotol Ratchet

- Public / Private Key pair doesn't work asynchronously
  - Just add more keys!
  - Root, Headers, Chain, Identity, Message Number
- When keys don't match, ratchet forward
- Establish next keys on read()
- Jen: https://github.com/trevp/axolotl/wikicurs

What Does 'It' Support?

- Encrypted messages
- Unencrypted messages
- Group Messaging
- MMS (audio, video, images)
- Can use any number for registration (i.e. burner)

How Does TextSecure Look

Interactive Part of the Talk

Padlock in message → Encrypted

Signal

UI is so god damn dead simple it's not worth wasting time discussing it

Note: Long-Term Identity Keys are in the contact user name (open the chat, hover over their name)

Conversations can be put into history

No encrypted database ATM.

COMSEC

- Caller reads the first word of the Short Authentication String
- Call recipient reads the second word of the SAS
- PFS is preserved so not possible to MiTM future calls
- Do it anyways to establish *duress*

RedPhone / Signal

Use the regular dialer on your phone.

Application will prompt you if the caller is using Redphone / Signal

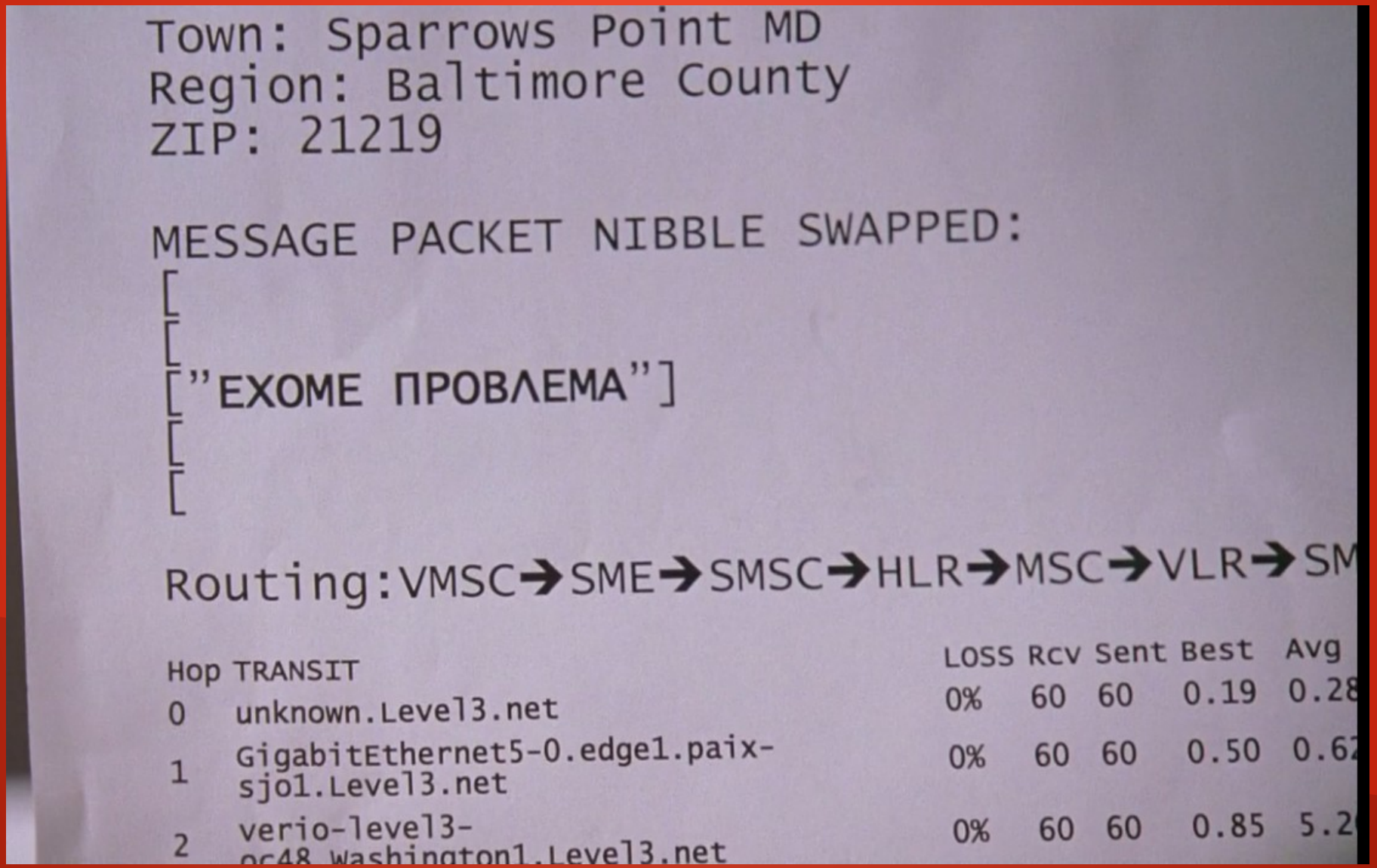
TroubleShooting

- Group MMS gets broken in TextSecure
  - Settings → Advanced → MMSC → URL
- Switch between encryption modes
  - SMS messages, long hold Press key
- Quick Close Database
  - Drag Down from the top

Future Work

- Remove encrypted SMS
- Merge TS / Redphone
- PR welcome
- Translations Welcome
- WhatsApp Integration
- TS servers (federated?)

Questions?


Town: Sparrows Point MD
Region: Baltimore County
ZIP: 21219
MESSAGE PACKET NIBBLE SWAPPED:
["EXOME ΠPOBΛEMA"]
Routing:VMSC→SME→SMSC→HLR→MSC→VLR→SM
Hop TRANSIT
LOSS Rcv Sent Best Avg
0 unknown.Level3.net
0% 60 60 0.19 0.28
1 GigabitEthernet5-0.edge1.paix-sjo1.Level3.net
0% 60 60 0.50 0.62
2 verio-level3-
0% 60 60 0.85 5.2