NSA PLAYSET: GSM

pierce , loki DEFCON 22

For the latest version of this presentation, check http://tinyurl.com/gsm2014

Who are we?

whois: Pierce

- 4th DEFCON as a speaker, always wireless
- 12th DEFCON as an attendee
- 10 years as InfoSec professional
- Currently working as a product security engineer

Who are we?

whois: Loki

- 12 years as a software developer and architect
- Currently specializing in data analytics
- Has always worn a security hat
- Interested in GSM for the past 4 years

Intro to GSM

- Most widely used cellular system in the world
- First to seriously consider security threats
- Originally developed during the late 1980s
- First deployed in the early 1990s
- Still in wide use today

Intro to GSM

- Uses A5/1 to communicate between handset and base station

History Lesson: 1994

- First attack on A5/1 Proposed

History Lesson: 2000

- Plaintext-required time-memory tradeoff attack

History Lesson: 2003

- Ciphertext-only time-memory tradeoff attack

History Lesson: 2007

- COPACOBANA
- H1kari demonstrates breaking A5/1 on FPGAs

History Lesson: 2008

- First tables generated, but never released
- A5/1 Cracking Project, Kraken, tables released

History Lesson: 2009

- A5/1 Cracking Project
- Kraken
- First Rainbow Tables Released

History Lesson: 2010

- Airprobe: GSM capture via USRP
- OsmocomBB: GSM capture via Calypso

History Lesson: 2011

- Something probably happened in 2011

History Lesson: 2012

- RTL-SDR: inexpensive SDR

History Lesson: 2013

- HackRF & BladeRF
  - improved inexpensive SDR

NSA Playset

- ease of use
- cost reduction

What We Did

- Airprobe working with multiple SDR platforms
- Airprobe signal tracking improved
- Kraken A5/1 in the cloud
- Bootable environment for capture

DEMO!

QUESTIONS?