Cross Layer Attacks and How to Use Them (for DNS Cache Poisoning, Device Tracking and More)

A research paper by Amit Klein

Introduction

- Random numbers – are they actually random?
- Linux pseudo-random number generator (PRNG)
- Prediction of future “random” numbers

DNS cache poisoning

- Backbone of the internet
- Importance makes it an attractive target
- Fairly old attack – set to rise in the future

DNS cache poisoning

- Attacker must guess connection parameters
- 31 bits of information must be known to spoof DNS answer
- Brute-force took 2 days
- Researchers performed the attack 3000-6000x faster

Device Tracking

- PRNG state can be extracted almost instantly
- Intercept traffic and identify victim
- Track victim across multiple sites and networks
- Operates on IP layer and above

Device Tracking

- Vulnerability deep within Linux kernel
- Doesn’t rely on IP fragmentation
- High speed – difficult for a human to stop

The Linux PRNG

- Per-core states – can change over time
- Made difficult by multiple cores, re-seeding, interrupts
- prandom_u32() – easy to count invocations
- Quick to determine internal PRNG state

Solving the PRNG state

- Linear equations over 113 unknowns
- Takes under 1 millisecond
- >=113 bits of PRNG output from victim
- Quick bursts use the same core

DNS cache poisoning - Step 1

- Learn PRNG core state of victim
- Burst of packets from victim
- Embedded HTML can force traffic

DNS cache poisoning - Step 2

- Predict source port of DNS query
- Core switching – must act quickly
- Much faster than brute force – can always retry

DNS cache poisoning - Step 3

- Send spoofed DNS answers
- Cover as many DNS ID values as possible
- Answer with correct ID will be accepted

Device tracking

- Relies on same principle – determine PRNG state
- Attack continues over time
- Must overcome core switching
- Repeat PRNG state extraction for multiple cores

Experiments and results

- 4.5 orders of magnitude faster than brute force
- Attack worked on 11/13 devices
- VPNs and incognito mode had no effect

Criticisms and suggestions

- Relies on PRNG output being externally visible
- Pre-image resistance
- Doesn’t work on most mobile networks – problem for android devices
- Prevented by port overriding

Thank you

Questions?