Mobile Network Challenges

(and why NANOG should care)

Joe Eggleston, Craig Labovitz
<joe,labovit>@arbor.net
Arbor Networks

Z. Morley Mao
zmao@eecs.umich.edu
University of Michigan

Observation

- **Little discussion about mobile at NANOG**
  - 1,870 emails about IPv6 in last year
  - And 11 emails about 3G / 4G
- **Possibly because…**

Observation

- **Little discussion about mobile at NANOG**
  - 1,870 emails about IPv6 in last year
  - And 11 emails about 3G / 4G
- **Possibly because…**
  a) Mobile networks are just not that important

Observation

- **Little discussion about mobile at NANOG**
  - 1,870 emails about IPv6 in last year
  - And 11 emails about 3G / 4G
- **Possibly because…**
  a) Mobile networks are just not that important
  b) 3G security and engineering are way better than fixed (i.e. no problems to discuss)

Observation

- **Little discussion about mobile at NANOG**
  - 1,870 emails about IPv6 in last year
  - And 11 emails about 3G / 4G
- **Possibly because…**
  a) Mobile networks are just not that important
  b) 3G security and engineering are way better than fixed (i.e. no problems to discuss)
  c) Mobile core is another group's problem (and they don't subscribe to NANOG)

Why NANOG Should Care

a) **Fixed line traffic is growing quickly**
   - Observatory data pegs fixed inter-domain at 45-55%
   - But mobile traffic growing 80-150% / year
   - Users want to access your network via a mobile connection.

b) **3G / 4G security is not better than fixed**
   - Likely far worse

c) **Organizational changes**
   - Mobile / fixed traditionally completely separate org
   - Almost 1/3 now merged or will merge in next year
   - Fixed-line security groups charged with securing mobile

So if you don't care now, you probably soon will.

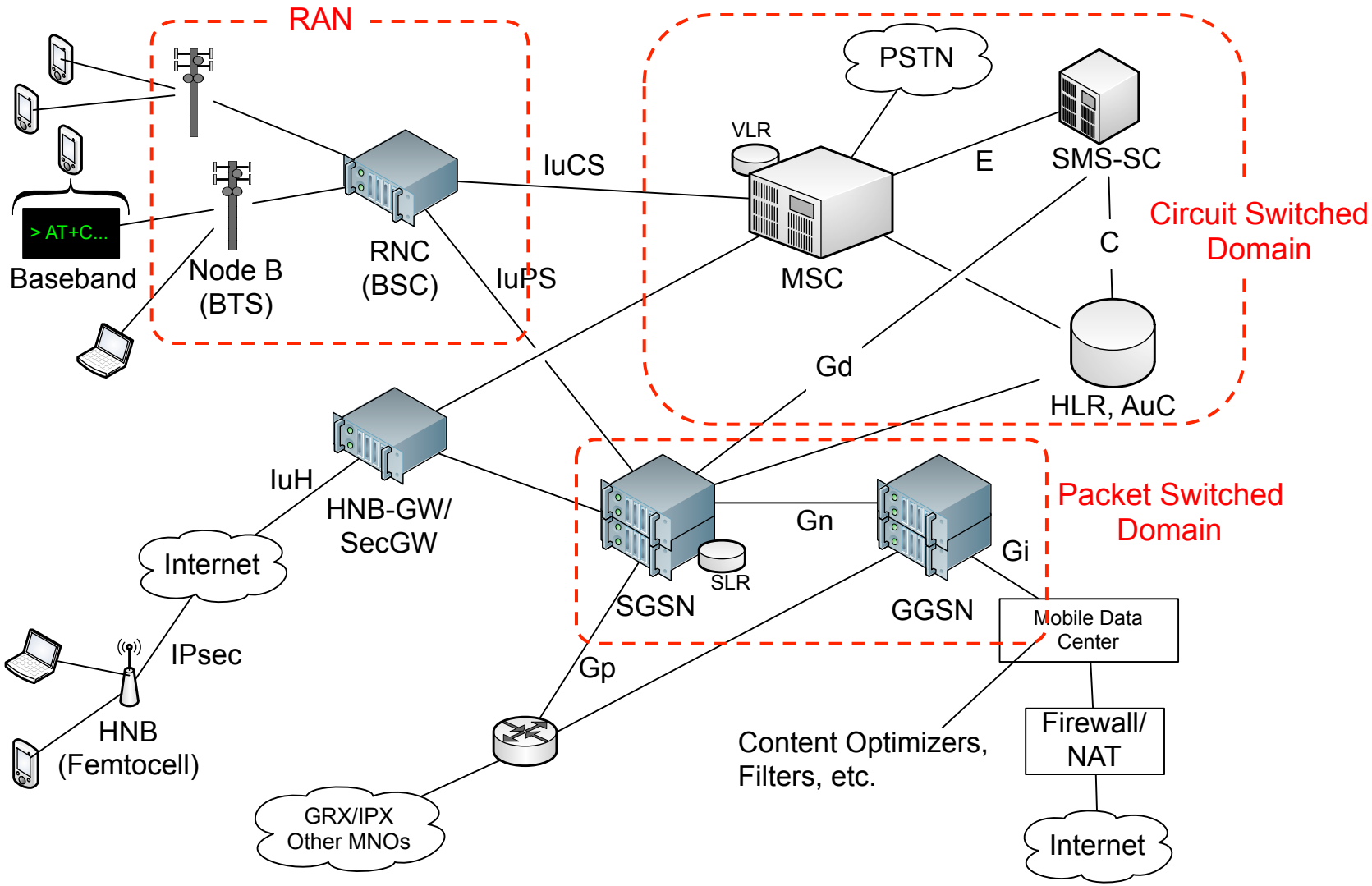
Agenda

- **Motivation**
- Engineering Challenges
- Security Challenges
- Questions

Why Mobile is Different

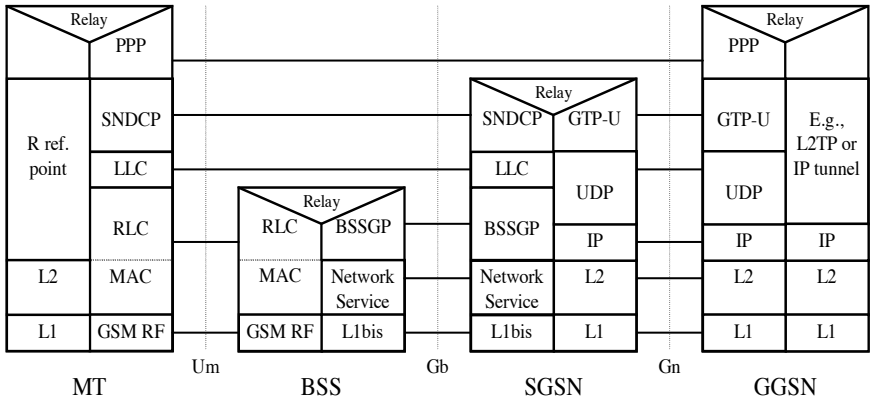
1. **Spectrum, Cell-sites, Backhaul, Battery**
   - Much of the cost
2. **Optimized for QoS, fine-grained billing, intelligence in the network**
   - Voice-centric assumptions (LTE vs. TD-LTE)
   - Latency
3. **Signaling load**
   - Incurs latency, strains infrastructure
   - Weak-link
4. **State tracking**
   - Intelligence in the network
   - Easy to attack (imagine a syn flood disabling a router)
5. **Complex, brittle protocols and stacks**
   - Massive specs, seldom used code paths, little scrutiny
   - TLVs within TLVs within TLVs
   - Result: buffer overrun cup runneth over

Mobile Network Review



Engineering Challenges

Challenge: Heavy-weight Architecture



GPRS Protocol Stacks

Source: 3GPP TS 23.060

The **mobile network contributes over 80% of the total latency** from a mobile device to Internet landmark servers.

See Huang et al. [1]

- **Network and phone architectural decisions have significant impact on performance**
- **Complex interactions between**
  - Phone
  - Network element buffering, retransmits
  - TCP

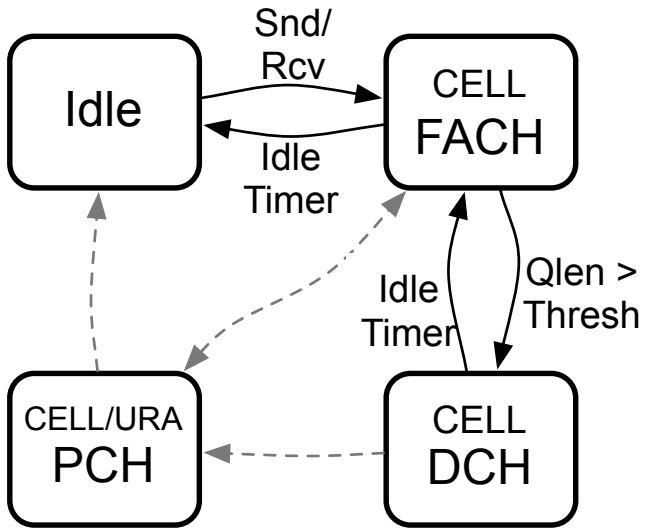
Challenge: Protocol/Network Interactions

```
PING 198.108.95.21 (198.108.95.21): 56 data bytes
64 bytes from 198.108.95.21: icmp_seq=0 ttl=52 time=2712.965 ms
64 bytes from 198.108.95.21: icmp_seq=1 ttl=52 time=215.452 ms
64 bytes from 198.108.95.21: icmp_seq=2 ttl=52 time=169.154 ms
64 bytes from 198.108.95.21: icmp_seq=3 ttl=52 time=146.524 ms
```

Transition from Idle to CELL_DCH
Joe's iPhone

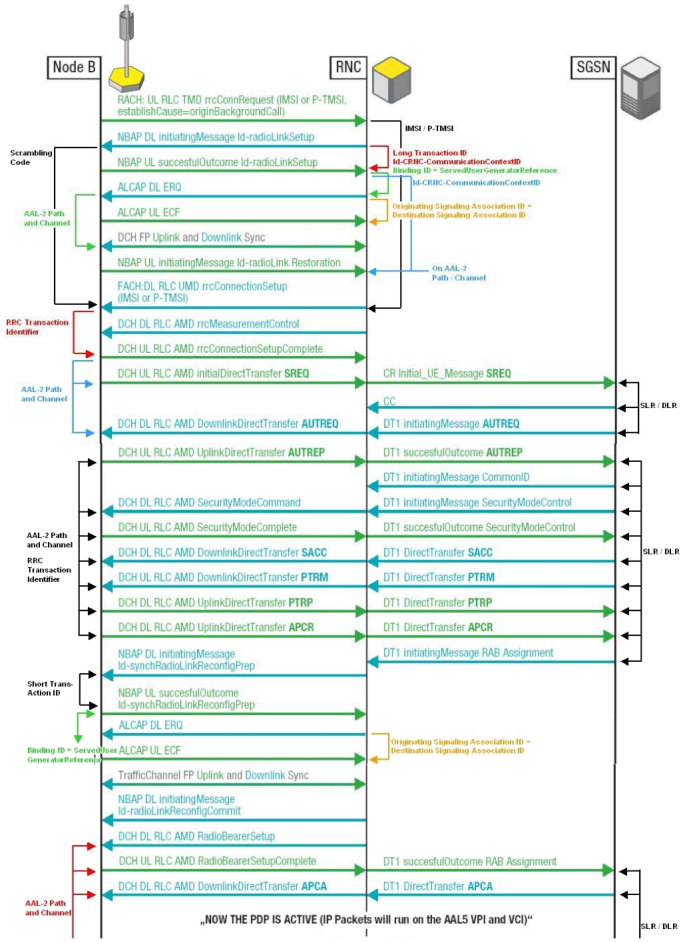
Channel-type Switching

- Remember TCP Tahoe, Reno, Vegas…?
- Now add a network with (configurable) states, timers, QoS classes…
  - All of which affect the bandwidth and latency
  - And can change underneath TCP

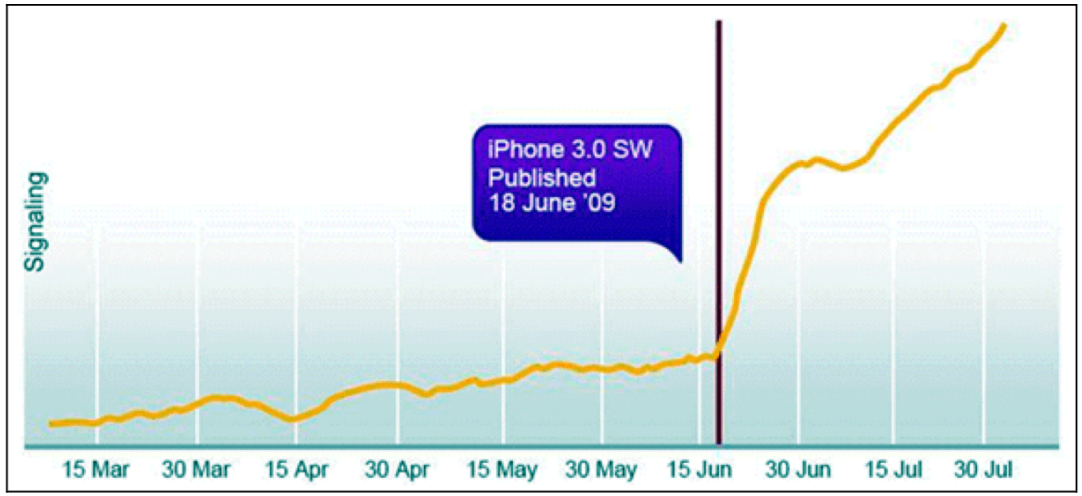


Radio Resource Control protocol states
See Qian et al. [2] and 3GPP TS 25.331

Challenge: Signaling Load



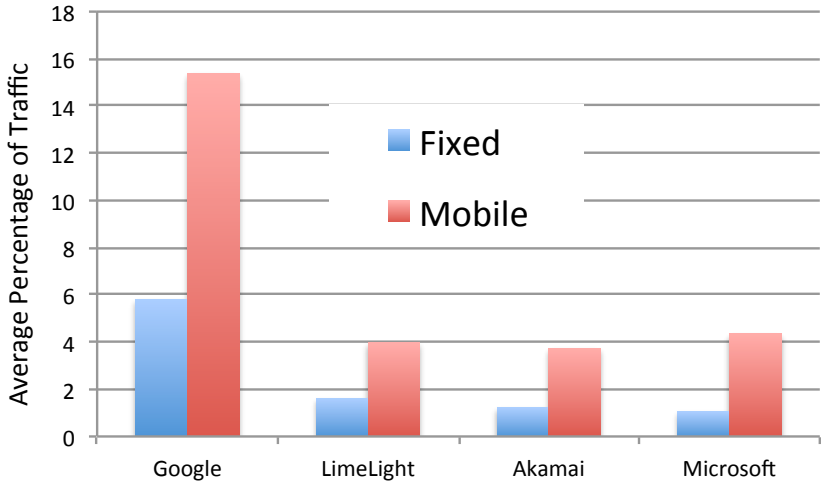
PDP-context Activation
Source: Tektronix

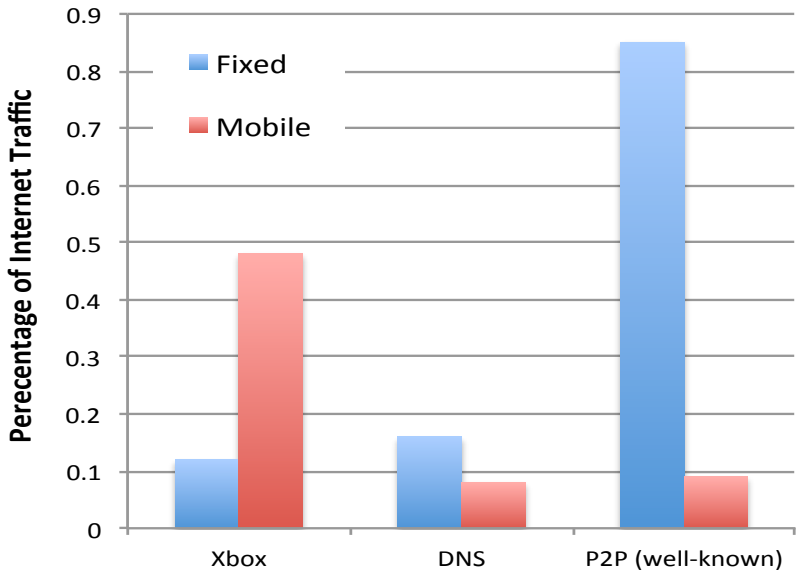


Source: Nokia Siemens Networks

- Even normal operation and vendor implementation decisions can create signaling load problems
- Control plane design provides broad attack surface

Challenge: Mobile Traffic is Different



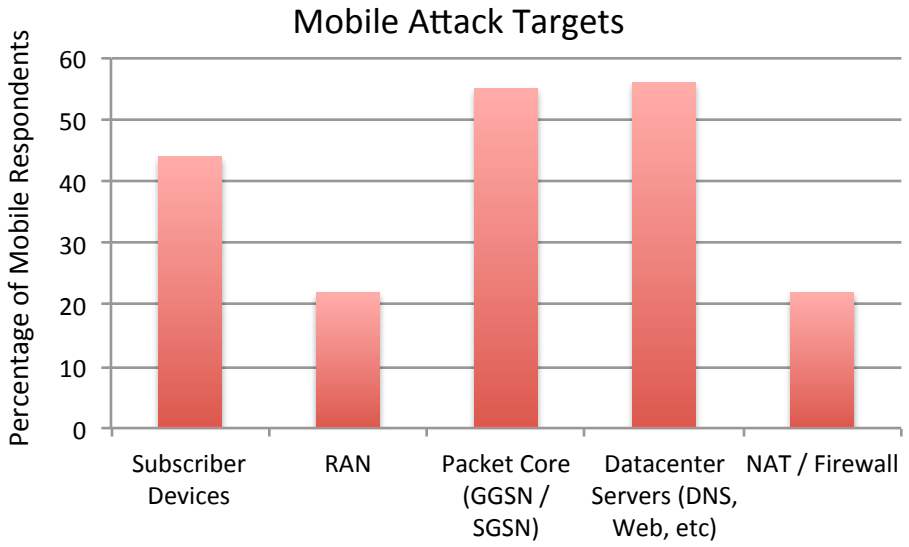


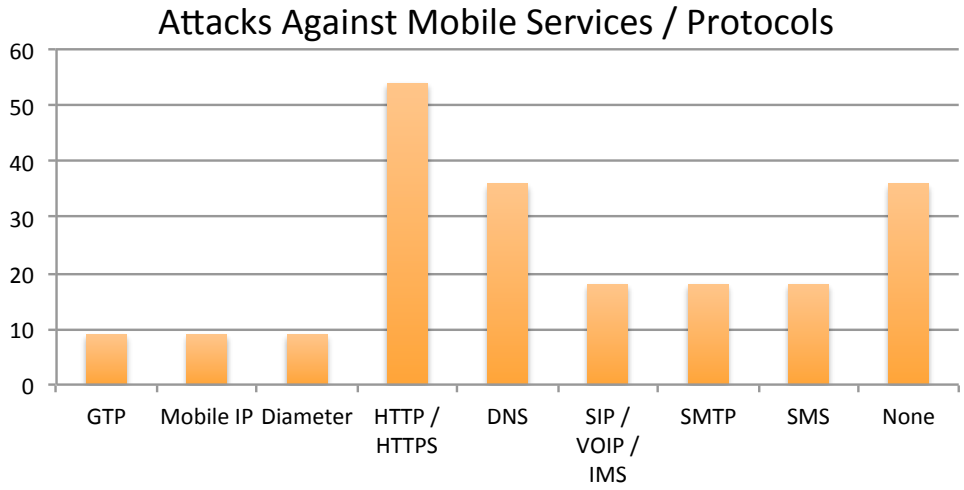
(ATLAS data)

- **2-3 times as much Google, Microsoft and CDN traffic from mobile than fixed**
  - Maybe makes sense for Google / MSFT
  - CDN?
- **Fraction of P2P**
  - Makes sense
- **5x as much Xbox in mobile?**

Security Challenges

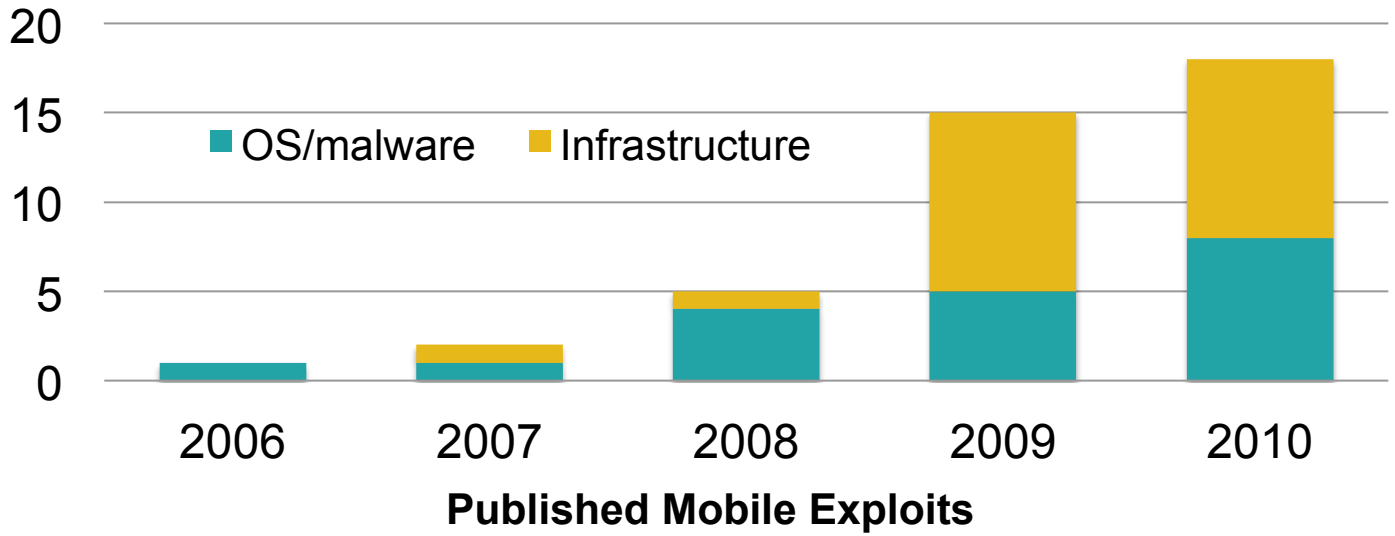
State of Mobile Security – Survey





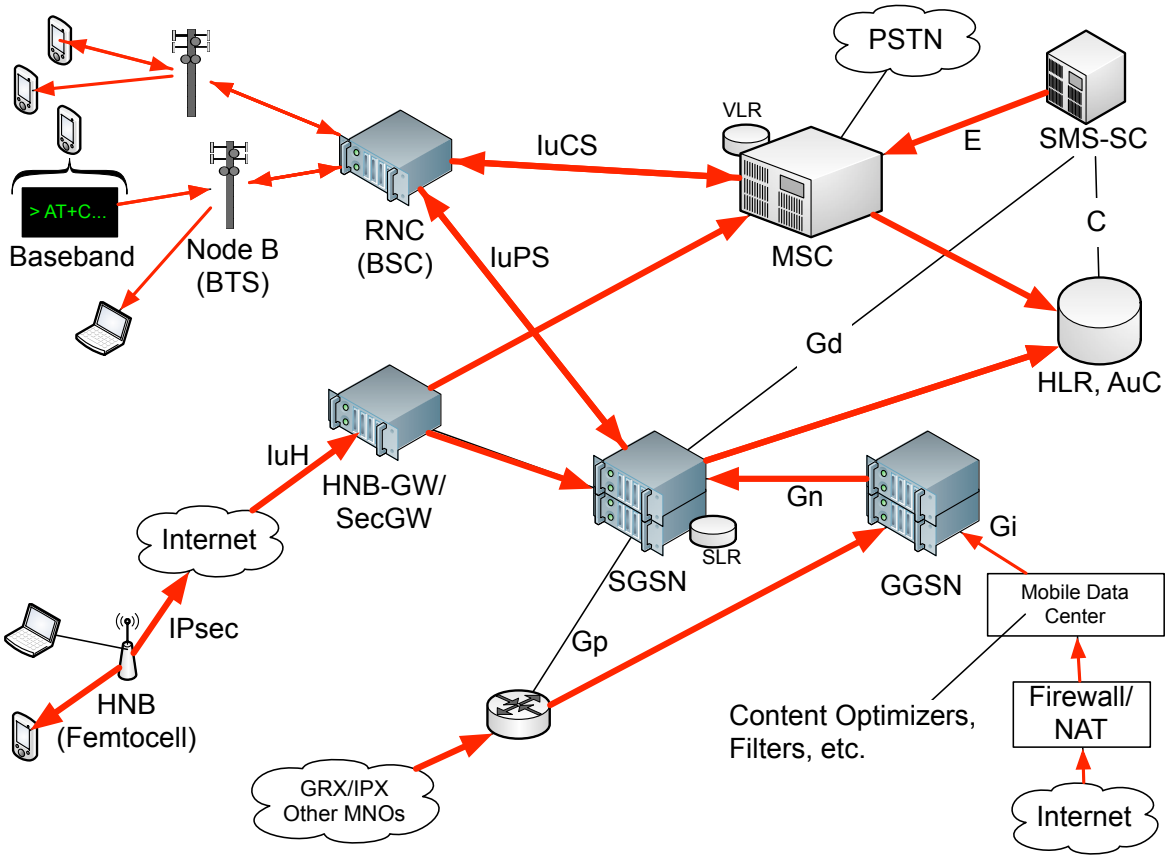
- 75% of MNOs say poor, bad, or non-existent mobile security / visibility
- More than half of mobile carriers have had outages in last year due to security event
- Broad range of attack targets within mobile network
- Mostly IP-level services targeted
  - Suspicion – security tools lacking elsewhere

State of Mobile Security – Changing Landscape



- **Barriers to entry are falling**
  - Internet C.W. – This is a good thing
  - Closed to open – Lots of SS7 interconnects and GRX peers
  - Cheap hardware – pico/femto cells, smart phones
  - Increasing scrutiny
- **More interesting target**
  - Data is cool, phone calls are boring

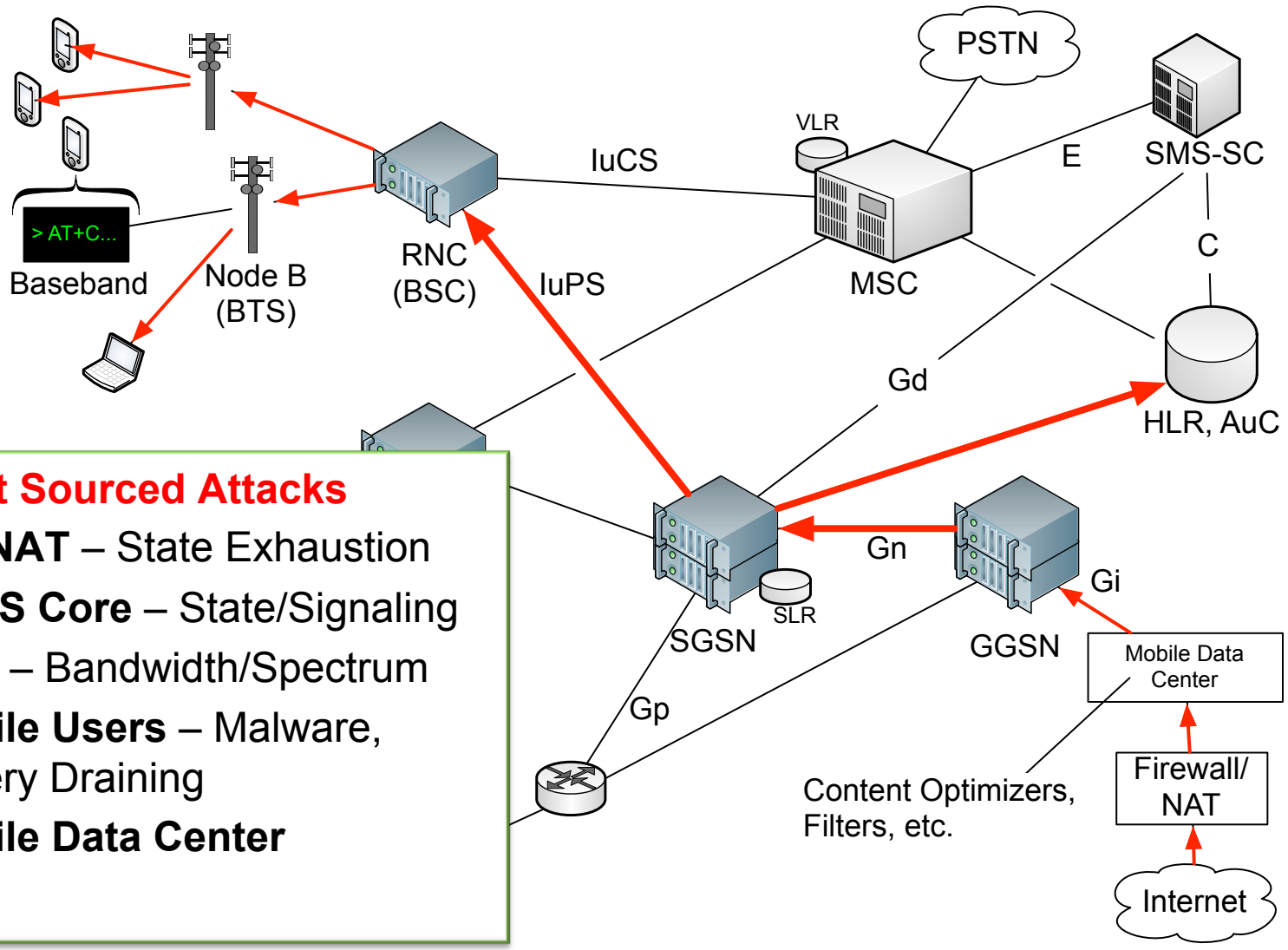
Mobile Security Attack Surface



Attack Surface

1. RF
   - Channel exhaustion
2. GPRS, PDP, Gn
3. HLR
   - Signaling DoS
4. GRX/IPX
   - DDoS, toll fraud, protocol interop
5. Gi
   - DDoS, worms, firewall evasion, state exhaustion, battery draining
6. Femtocells
7. SMS
8. SIGTRAN, SS7
9. Mobile to Mobile
10. Weak/broken crypto

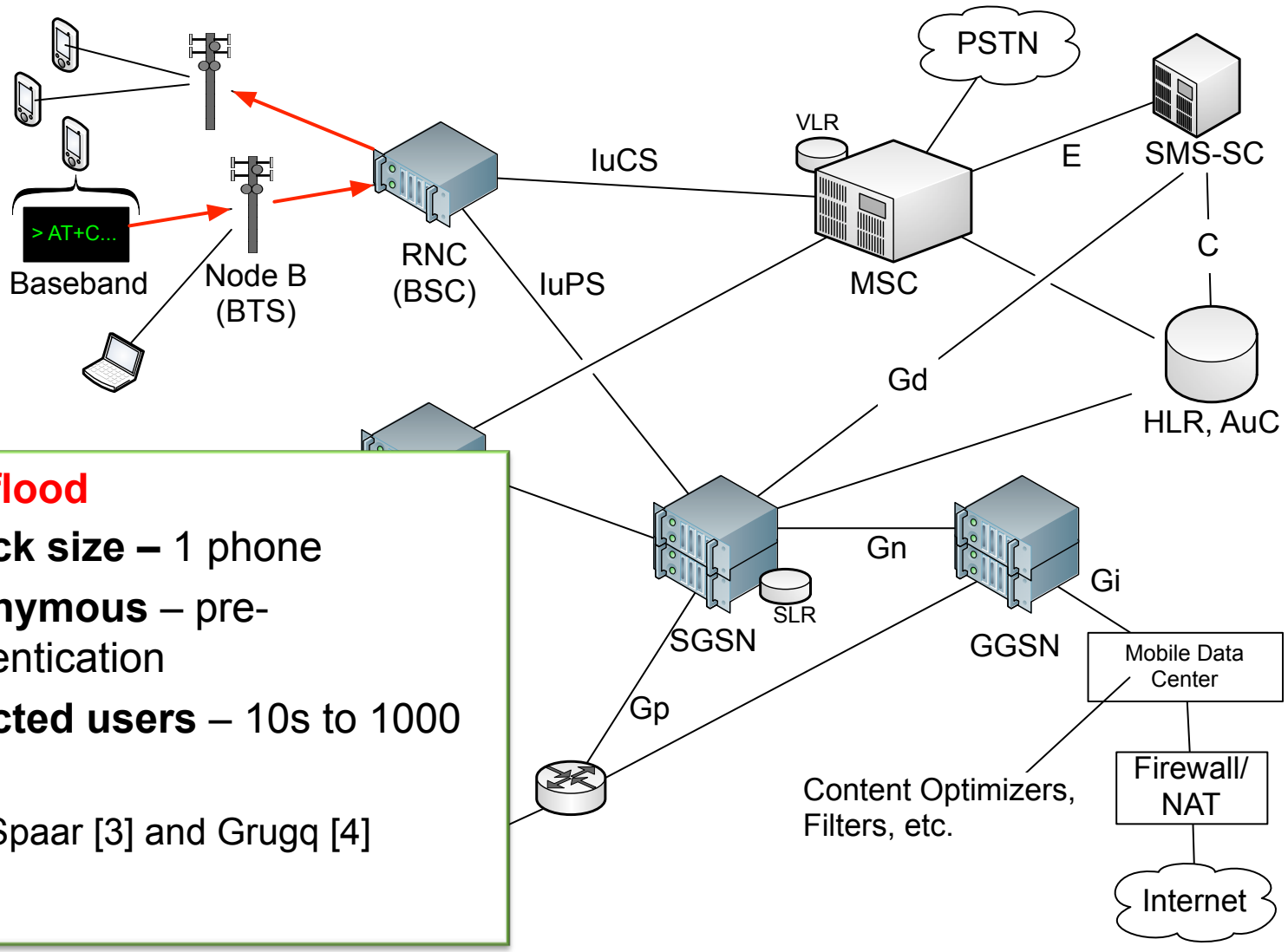
Threats: Gi



Internet Sourced Attacks

- **FW/NAT** – State Exhaustion
- **GPRS Core** – State/Signaling
- **RAN** – Bandwidth/Spectrum
- **Mobile Users** – Malware, Battery Draining
- **Mobile Data Center**

Threats: Signaling Attacks (RF)



RACH flood

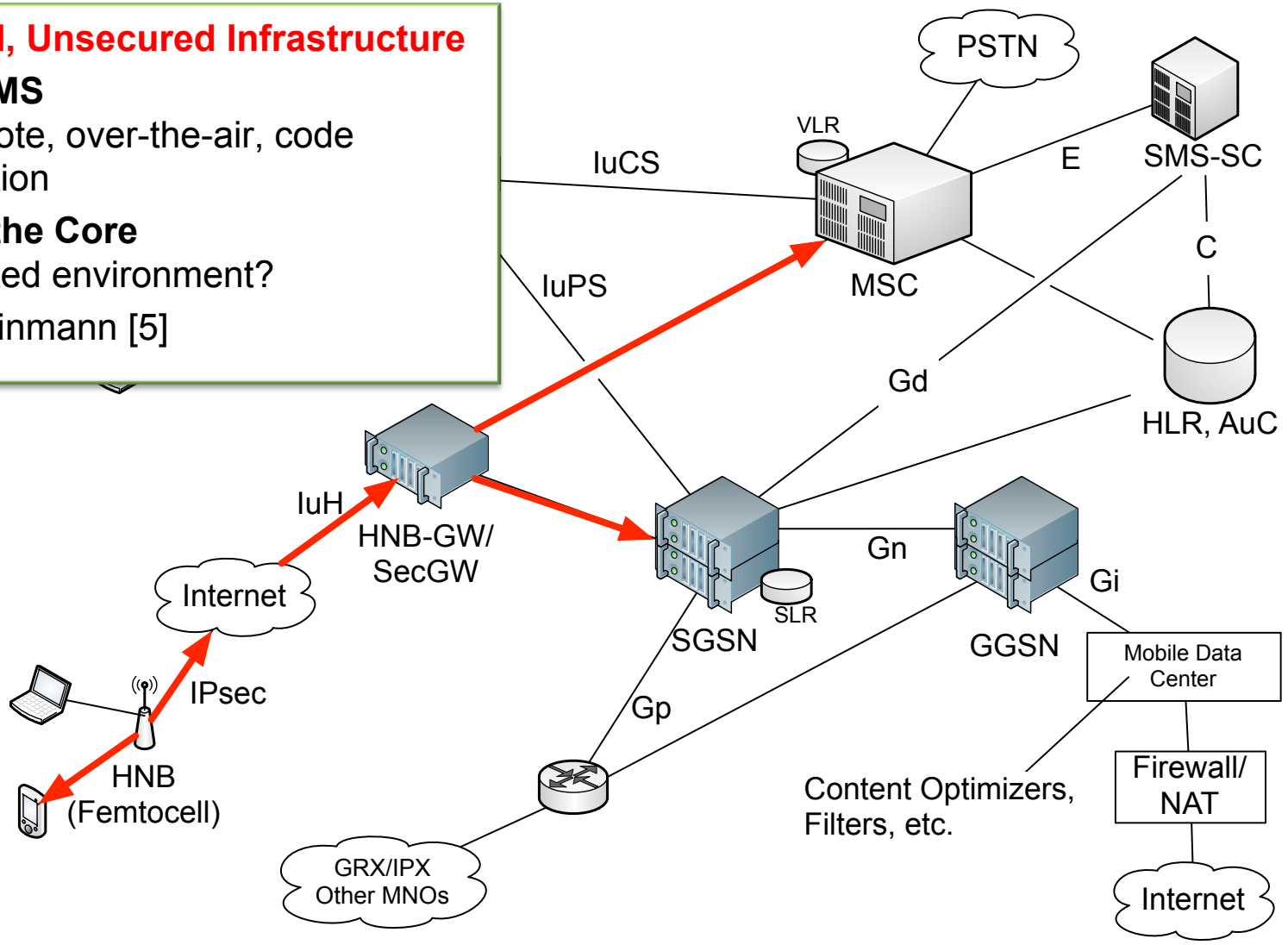
- **Attack size –** 1 phone
- **Anonymous** – pre-authentication
- **Affected users** – 10s to 1000

- See Spaar [3] and Grugq [4]

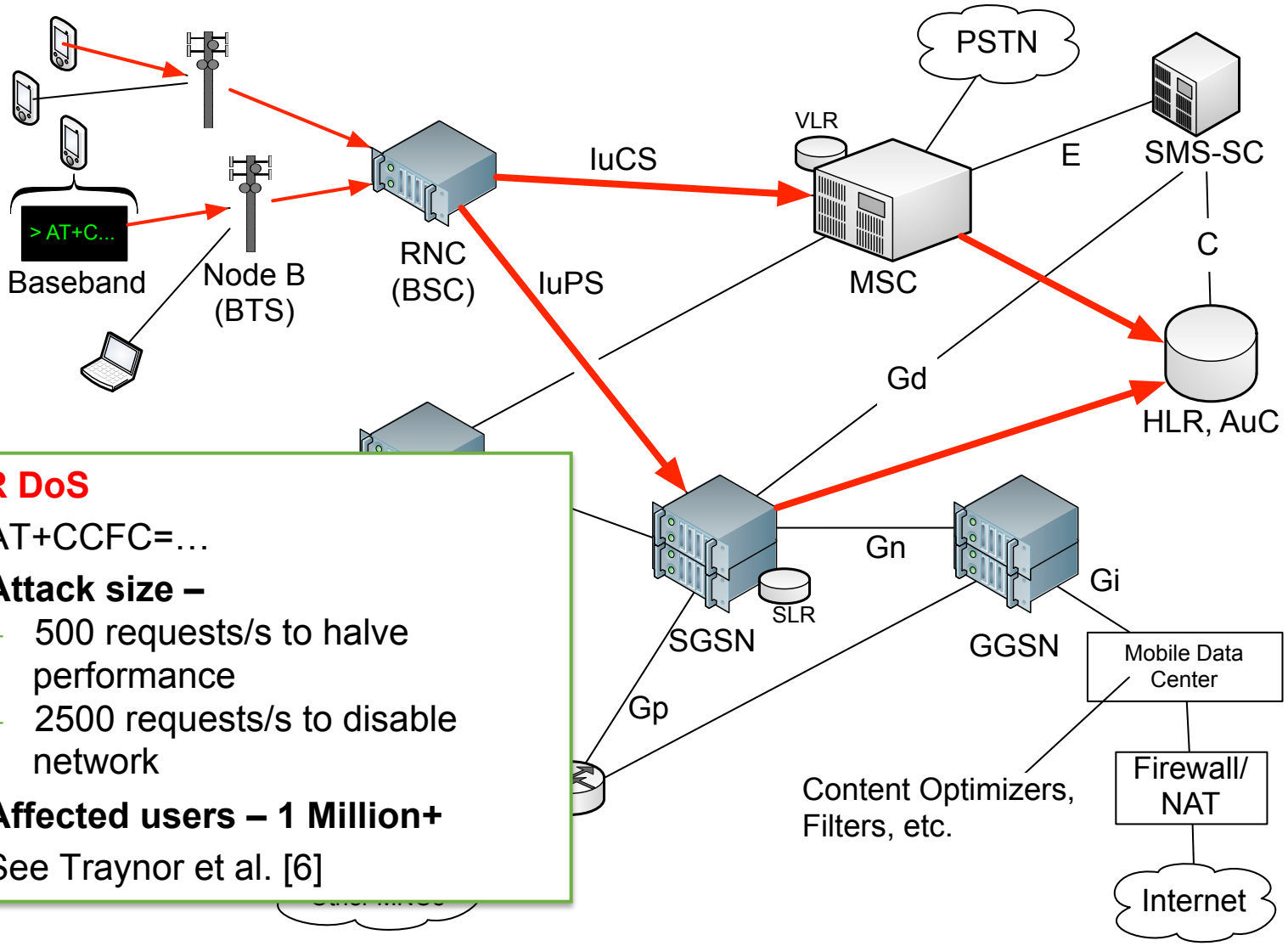
Threats: Femtocells, Rogue Base Stations

Authorized, Unsecured Infrastructure

- **Attack MS**
  - Remote, over-the-air, code injection
- **Attack the Core**
  - Trusted environment?
- See Weinmann [5]



Threats: Core Signaling



HLR DoS

- AT+CCFC=…
- **Attack size –**
  - 500 requests/s to halve performance
  - 2500 requests/s to disable network
- **Affected users – 1 Million+**
- See Traynor et al. [6]

Summary

- **Mobile traffic is different from fixed-line**
  - Exhibits unique characteristics / trends
- **Mobile security is vastly different from fixed line**
  - Especially with respect to maturity / tools
- **Strong mismatch between mobile conventional security / engineering wisdom and emerging realities**
- **Still in the very early days of mobile**
  - Smart phones small percentage of market
  - Only now seeing significant research and engineering evaluation of mobile security

More Information

- **3GPP**
  - http://www.3gpp.org/
  - Mailing lists – http://list.etsi.org/
  - Focus on specs
- **GSMA**
  - Proprietary – participation requires (expensive) membership
- **Osmocom**
  - http://www.osmocom.org/
  - Amazing open source project. Building all the pieces of a mobile network.
  - Focus on developing
- **For further discussion**
  - mailto:mnog-join@mnog.org

Questions?

Joe Eggleston
joe@arbor.net

Craig Labovitz
labovit@arbor.net
http://www.monkey.org/~labovit

Z. Morley Mao
zmao@eecs.umich.edu

References

[1] *Anatomizing Application Performance Differences on Smartphones*, Huang et al., Proceedings of ACM MobiSys, 2010

[2] *Characterizing Radio Resource Allocation for 3G Networks*, Qian et al., Proceedings of Internet Measurement Conference, 2010

[3] *A Practical DoS Attack to the GSM Network*, Spaar, Deepsec, 2009.

[4] *Base Jumping: Attacking GSM Base Station Systems and mobile phone Base Bands,* Grugq, Blackhat USA, 2010.

[5] *The Baseband Apocalypse*, Weinman, 27C3, 2010.

[6] *On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core*, Traynor et al., Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 2009.