Architectural Challenges

Arun Venkataramani
Univ. Massachusetts Amherst
arun@cs.umass.edu
Architecture: **Design Goals**

1. **Host + network mobility**
2. No global root of trust
3. Intentional data receipt
4. Byzantine robustness
5. **Content addressability**
6. Evolvable network
Naming and Addressing
Location Service: **Scalability to billions of mobiles**

- **Function:** Resolve Host → [NA1, NA2,...]
- **Scale:** 10B devices, 100 networks/day ⇔ 10M/sec
Location Service: **Scalability to billions of mobiles**

- **Function:** Resolve Host $\rightarrow$ [NA1, NA2,...]
- **Scale:** 10B devices, 100 networks/day $\leftrightarrow$ 10M/sec

---

**NSF FIA MobilityFirst Project - EAB Meeting Feb 28, 2011**
Location Service: **Scalability to billions of mobiles**

- **Function:** Resolve Host $\rightarrow$ [NA$_1$, NA$_2$, ...]
- **Scale:** 10B devices, 100 networks/day $\leftrightarrow$ 10M/sec

- **Metrics:**
  1. Query/Update delay (<50ms)
  2. Response staleness (<500ms)
  3. Load balance
  4. Fault tolerance
Location Service: **Mechanisms and tradeoffs**

1. Consistent hashing
   - Load balance, fault-tolerance
   - Proximity

2. Replication
   - Proximity
   - Update bandwidth

3. Caching
   - Proximity
   - Staleness

NSF FIA MobilityFirst Project - EAB Meeting  Feb 28, 2011
Location Service: Scalability to billions of mobiles

- **Function**: Resolve Host → [NA₁, NA₂,...]
- **Scale**: 10B devices, 100 networks/day ⇔ 10M/sec

**Design issues:**
1. In-situ routing deflection (?)
2. Structured local scope IDs (?)
3. Network anycast to root servers
4. Context-based addressing
Location Service: Content

**Function:** Resolve Content $\rightarrow [NA_1:HA_1, NA_2:HA_2, \ldots]$, where HA$_i$‘s are authoritative content trackers

**Design challenges:**
1. Proximate content retrieval
2. Traffic engineering flexibility
3. Storage-aware routing using opportunistic caching/retrieval

NSF FIA MobilityFirst Project - EAB Meeting  Feb 28, 2011
Security
Architecture: Design Goals

1. Host + network mobility
2. No global root of trust
3. Intentional data receipt
4. Byzantine robustness
5. Content addressability
6. Evolvable network
Security: Hijack/Spoof tolerance

- Self-certifying GID = public key

1. Bob’s human readable name
2. Bob’s GID, NA
3. Send Alice’s handshake data signed by Alice’s GID to Bob’s NA
4. Name certification + location service
5. Send Bob’s handshake data signed by Bob’s GID to Alice’s NA
6. Verify using Bob’s GID

NSF FIA MobilityFirst Project - EAB Meeting  Feb 28, 2011
Security: Decentralizing Trust in Naming

- **Goal:** No single root of trust in name certification

- **Approach:**
  - Multiple name service providers (NSP)
  - Many-to-many mapping from namespaces to NSPs
  - Quorum-based certification
Security: **No single point of subversion**

**Goal:** Scalably tolerating Byzantine faults for naming, routing

**Approach:**

- **Naming:**
  - BFT throughput scalability wrt faults and number of servers
  - Geographic scaling support
  - BFT within and across name service providers

- **Routing**
  - Securable protocol design, eg, consensus interdomain routing, by identifying safety and liveness properties
  - Multipath + management plane for data plane security
  - Integration with naming, management plane, and intradomain routing
Security: Intentional receipt for DDoS

Goal: Scalable fair resource allocation with intentional data receipt

Approach:
- Packets carry unspoofable congestion policing feedback
- Congested routers use pair-wise keys for congestion policing feedback that receivers use as capability tokens
- Access routers police senders’ traffic to guarantee per-sender fairness without per-sender queues
Privacy Challenges

Goal: Quantifiable privacy

Approach: Identifying privacy concerns:
- Host identifiers allow linking traffic to specific devices
- Self-certifying addresses reduce plausible deniability
- Lookup service could enable geo-tracking by third parties

Privacy Mechanisms

- Allow Home Agent Redirection
- Lookup Service
- NA:HA
- Allow HA Pseudonyms
- Home Agent
- AS 1
- AS 2
- Hospital
- HA swaps pseudonym
Conclusions/Questions