

Not-a-Bot: Improving Service Availability in the Face of Botnet Attacks

Ramakrishna Gummadi, Hari Balakrishnan, Petros Maniatis, Sylvia Ratnasamy

And other client-side defenses
Presented by Paul Pearce

The Threat

- Bots are a generic crime platform
- Bots are responsible for:
 - > 85% of spam email
 - 14-20% of ad clicks
 - > 4000 DDoS web attacks per week
- How to separate bot from human behavior?
 - Can it be done at the granularity of requests?

Current Defense

- Require explicit human input
 - Ex CAPTCHAs

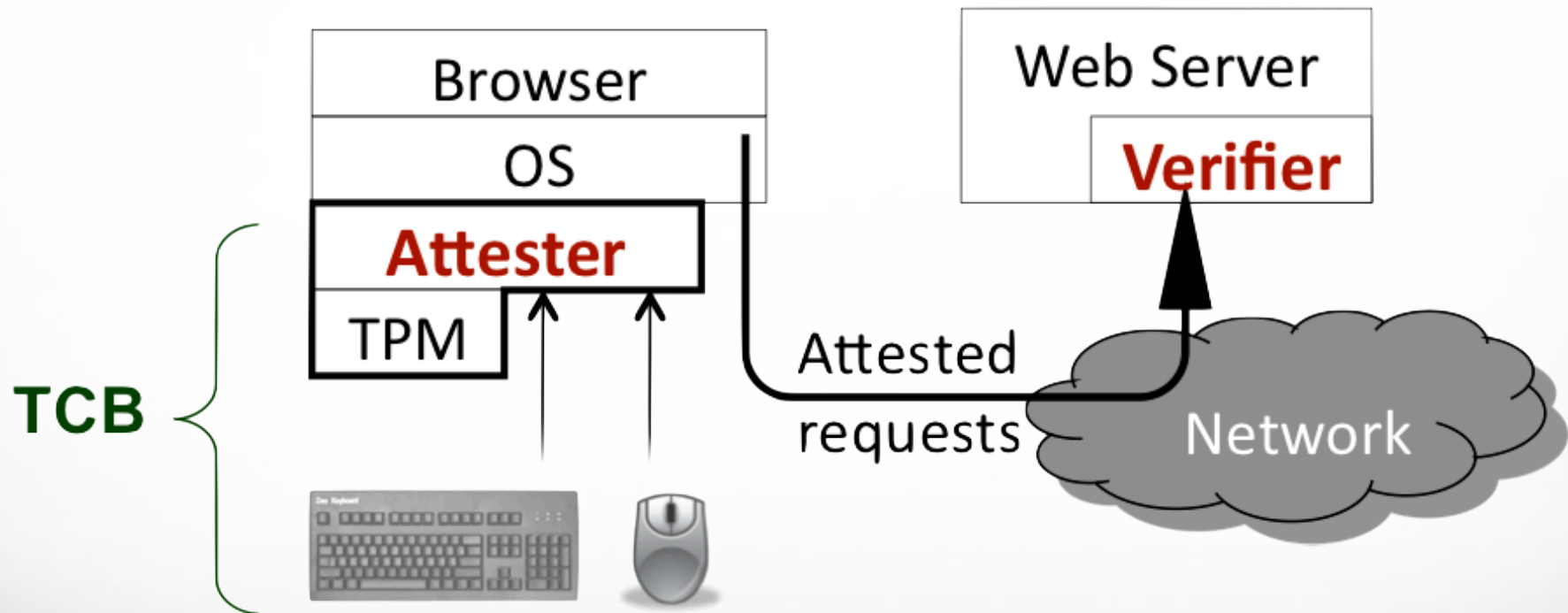
Anc *dalsist* *UNEK*
valite *difne* *sonated*
pliom *Unbacher* *uphadeci*
Agunt *gijie* *ummedar*
cardho *knopperb* *ZUMMS*



Not-a-Bot (NAB)

- Key insights
 - Humans use a keyboard and mouse, bots don't
 - Humans are slow, bots aren't
- Add trusted module to the client (Attester)
 - Monitor keyboard and mouse for activity
 - Cryptographically sign request if it corresponds to human activity
- Goal: Limit (not eliminate) bot generated requests

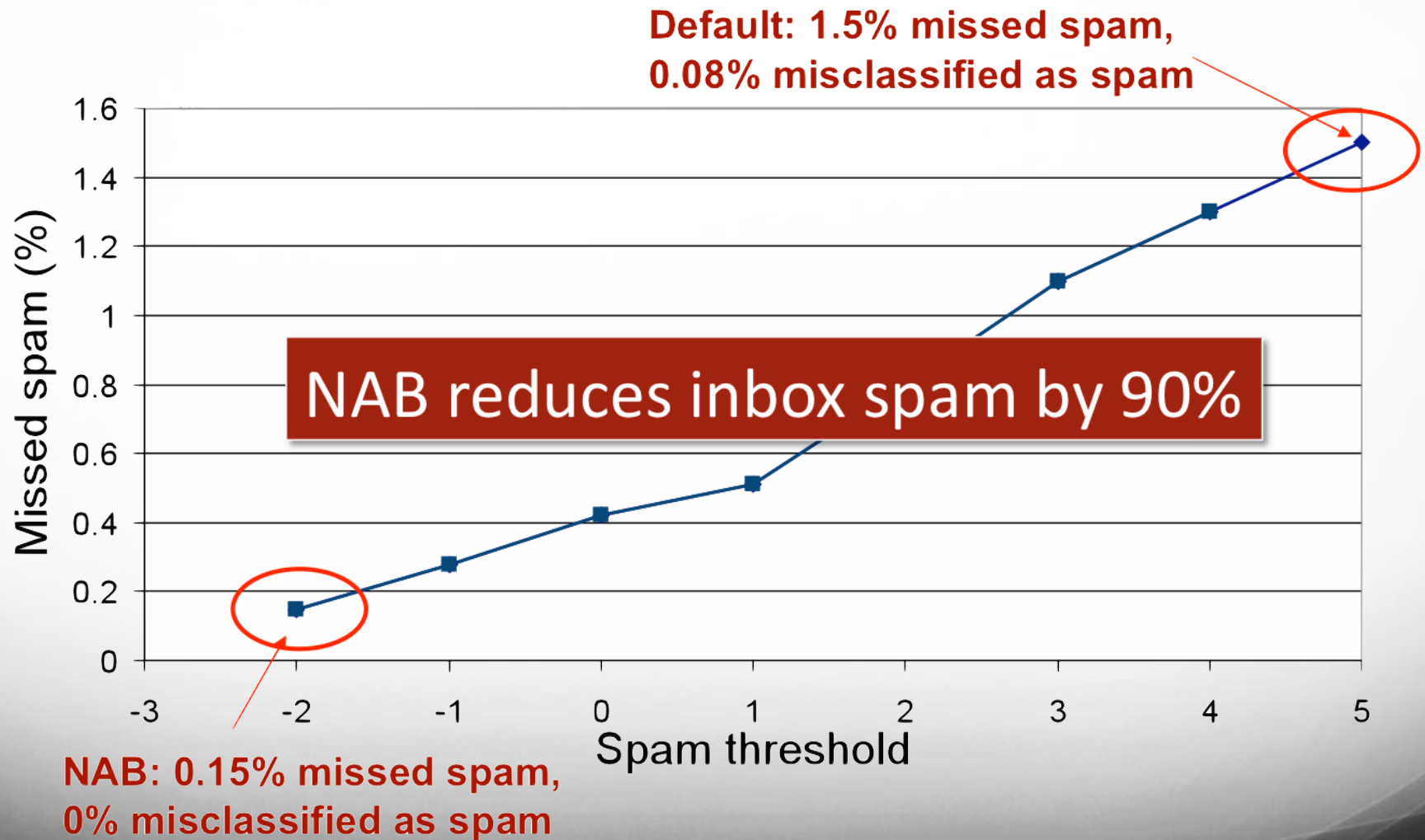
Design



Details

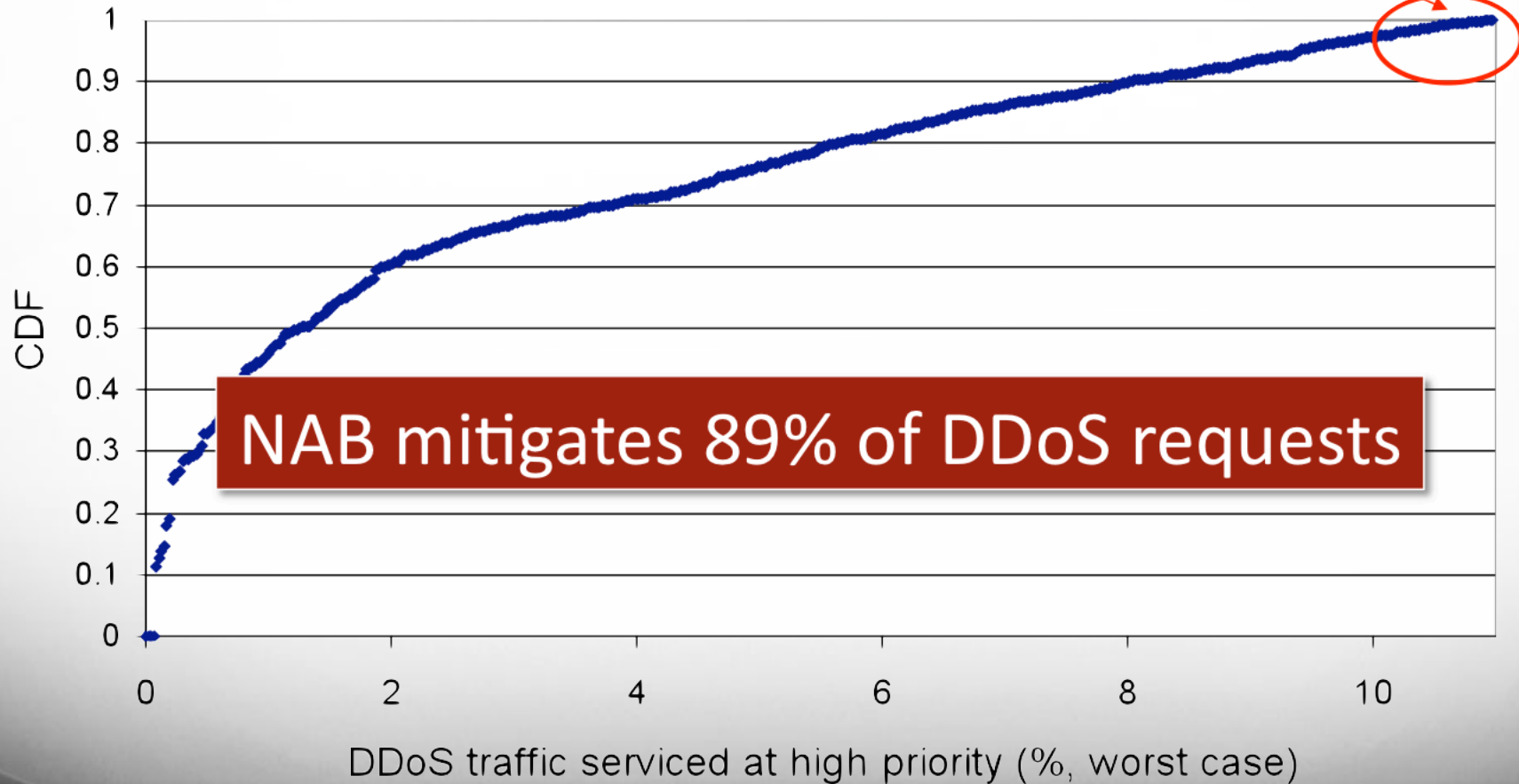
- Prototype implemented as Xen module
 - TPM used to assure attester integrity
 - Direct Anonymous Attestation (DAA) to assure privacy
 - Simple time Δ scheme
 - Supports HTTP and SMTP
- Requires modification of both client and server applications
 - No protocol changes
- Evaluated on real-world user and bot traces
 - No False Positives!

Spam Mitigation



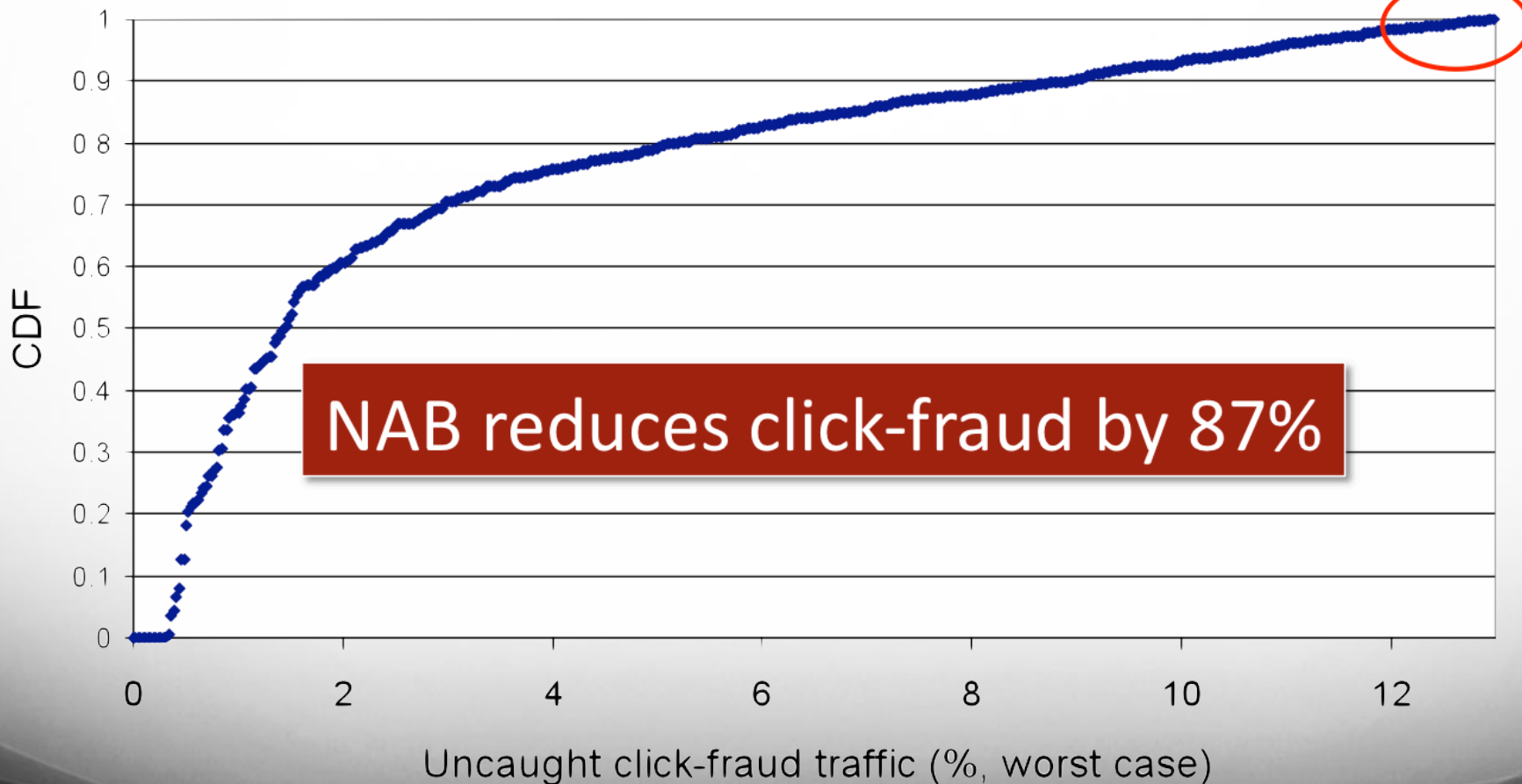
DDoS Mitigation

No trace sees more than 11% prioritized DDoS



Click-Fraud Mitigation

No trace sees more than 13% click-fraud traffic



Problems

- ~10ms compute time per attestation
 - Verification is less costly
- Non-trivial architectural changes
- Narrow threat mitigation
 - Does not prevent data theft
- Potential arms race

Client-Side Defense

- “Holding the Internet Accountable,” David Andersen et al.
 - Key insight: owners of compromised machines aren’t malicious
 - Custom network hardware to enable “Shut-Off Packets” (SOPs)
- Both NAB and SOPs leverage owner intent to stop attacks at their source
- Virtual Dedicated Clients?

Client-Side Defense Discussion

- Is pushing the problem into the client system the right answer?