Poster Abstract: A secure P2P SIP system with SPAM prevention

Joakim Koskela *joakim.koskela@hiit.fi*
Juho Heikkilä *juho.heikkila@hiit.fi*
Andrei Gurtov *gurtov@hiit.fi*
Helsinki Institute for Information Technology

I. Introduction

The Internet is plagued by an increasing number of nuisances ranging from simple inconveniences to threats, such as phishing and identity theft. The scale of these problems has grown to alarming proportions, as well seen in the amount of unsolicited electronic mail (SPAM) in the Internet today.

In systems where the control lies in trusted centralized entities threats have been well recognized, and techniques developed to mitigate the effect. However, as mobile and ad-hoc networks are becoming commonplace, we see more systems designed using distributed and peer-to-peer architectures. A similar outbreak of security threats is feared in these domains, unless we integrate security in the design. The mechanisms developed for centralized systems might not be applicable, forcing us to explore new methods and models.

Our work focuses on developing and experimenting with security mechanisms for distributed real-time communication systems. We concentrate on issues such as secure architecture, privacy and identity management, as well as prevention of unwanted calls.

II. System architecture

The basis for our experiments is a Host Identity Protocol [1, 2] (HIP)-based peer-to-peer overlay framework, used in conjunction with SIP-based instant messaging (IM), video- and voice over IP (VoIP) clients to create a peer-to-peer SIP (P2PSIP [3]) prototype. Unlike most other P2PSIP initiatives, we do not concentrate on constructing the overlay, but rather on the security issues after it is set up. An overview of the system is depicted in Figure 1. The implementation is currently run on the Linux-based Nokia N810 Internet tablets to conduct user trials.

By using HIP for the peer-to-peer connections, we achieve strong authentication and confidentiality, mobility, multihoming and NAT traversal even in networks with limited or no access to the Internet or infrastructure. Strong identities are achieved using public key certification scheme, where identities are tied to keys, certified by a trusted authority. The identity keys are used to certify the registration information published by peers to one or more *storage services*. This information is sought by peers when establishing connections, as it contains the contact information (location and HIP-related information) needed to establish a HIP-based peer-to-peer connection.

The system can easily use any storage service that offers a hash table interface, whether centralized, distributed or completely based on a peer-to-peer overlay network [4]. As the registration information is certified, even untrustworthy networks can be utilized. The use of these storage services is modular, and currently the system supports, concurrently, LAN multicast (for local networks) and a number of DHT-service interfaces (including OpenDHT).

Privacy extensions based on public key cryptography and key obfuscation have also been developed which hide the content and publisher of the registration packages. This prevents intermediate nodes in the overlay from tracking the calls made through the system.

III. Preventing SPAM calls

To filter out calls from total strangers, especially Spam over IP Telephony (SPIT), we have implemented a locally trusted path-finding service, which maintains a database of anonymized contact lists. Our system differs from e.g. Ostra [5] in that it is non-intrusive in that it does not require the users to evaluate others, simply share their contacts with a trusted party. The main idea behind the service is to build a privacy protecting view to the social network beyond the first step. As people might not want to share their contacts (even in an anonymized form) with all their contacts, a party that keeps the information confidential but provides path descriptions can help.

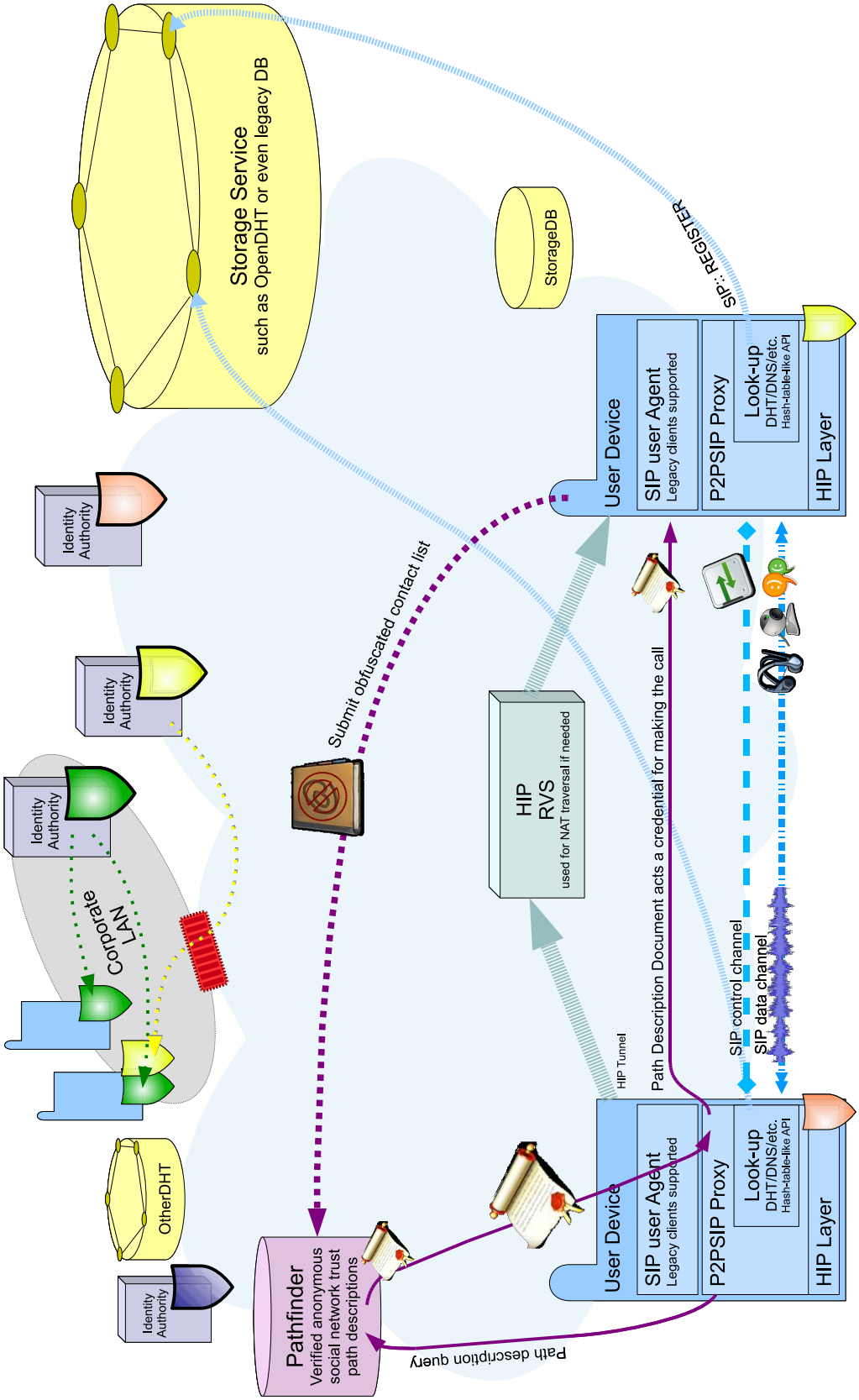

Figure 1: The components of the P2PSIP system with SPAM prevention. In addition to the users and peers, identity authorities, Pathfinders and storage services (possibly peer-to-peer overlays) can be present. The Pathfinders are used to provide trust-based credentials which are provided when establishing the HIP-based peer-to-peer connections.

The recipient proxy may contain various access rules for the caller. These rules can depend on the presence settings, from allowing only certain contacts to call, to allowing anyone to call. For the median rules, allowing only friends of friends to call, or two or more hops away people to call, the proxy can require the caller to provide a path statement from a trusted database. Currently the path description contains the length of the path allowing to filter out callers too far away in the social network, but future versions may include weighted links or descriptive metadata.

The balance between privacy and reputation is an important part of our research. The service is implemented as freely deployable stand-alone HTTP server, which can be found using the overlay. The service itself currently relies on traditional HTTP queries, so using the overlay is not a requirement as such. This will allow for decentralization and distribution based on real world trust issues, rather than building either a global centralized service or overly amount of transparency in distributed network where privacy is weak.

IV. Performance evaluation

To evaluate the feasibility of our system for a wide deployments on mobile, resource-limited devices, we measured the Post Dial Delay on Nokia N810 Internet tablets and examined the scalability of our Pathfinder model.

IV.A. Post Dial Delay

Post dial delay (PDD), the time interval between the caller dialing and receiving a dial tone indicating the status of the call (ringing, busy or abandoned), is commonly used to express the efficiency of telephone systems. We recorded 30 samples between peers with no previous relationship, and 50 after a connection had been made (presented, separated into the most important components, in figures 2 and 3).

As Figure 2 shows, the prototype, when used on the hand-held Internet tablets, introduces a significant delay in the call set-up times, caused mostly by the initial HIP handshake (base-exchange, BEX) between two peers. However, the performance does not suffer from the use of HIP during transport, as the effect of the IPSec encryption is minor [6], even on the low-performance mobile devices. The performance of the distributed storage can naturally affect the call set-up times significantly, although server-like, or better, lookup times can be achieved using robust overlay algorithms.

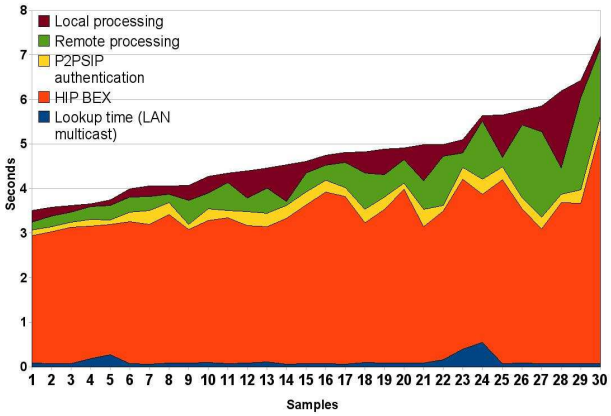

Figure 2: Post dial delay, broken into components and sorted by total duration, on Nokia N810 Internet tablets when establishing new peer connections.

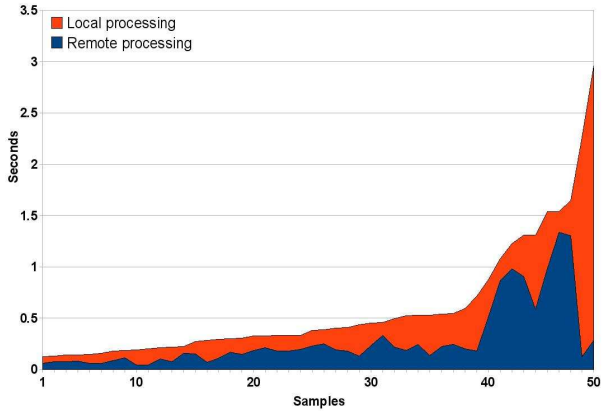

Figure 3: Post dial delay, broken into components and sorted by total duration, on Nokia N810 Internet tablets when using previously established peer connections.

Figure 3 shows the PDD after the initial P2P connection has been established. Local and remote processing denotes the time spent processing SIP messages and communicating with the SIP UA on the local and remote peer. The large variation in the processing times can be explained by their high dependency on the SIP UA, which is easily influenced by state of other processes running on the device. Aside from the BEX, done only once between two peers, the performance of the system is satisfactory, with the PDD for the majority of calls being below 0.5 seconds, and never over 3 seconds.

IV.B. Pathfinder performance

We ran performance tests on our two-way-search-based service using the social network formed by PGP key signatures. This so-called web of trust is a net-

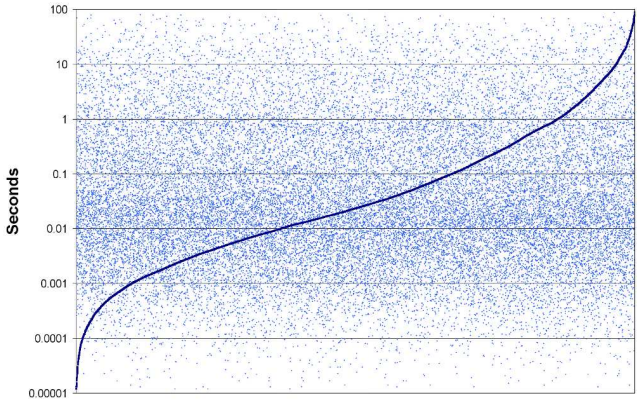

Figure 4: Performance test on the pathfinder implementation. Queries for 30 000 random-to-random paths of maximum of 6 hops. Shown both in measurement order (cloud) and sorted by time (curve).

work of over 35 000 nodes and nearly 400 000 links (signatures). Results in Figure 4 exhibit how wide the time scale needed to find a path is. The median result is 23 ms. However, browsing through large number of nodes can take tens of seconds. This can partially be remedied by using a sensible maximum path length as paths longer than 3 or 4 steps provide little value to the user. Consider that six degrees of separation would theoretically reach any person on Earth [7]. However, the search time correlates more with the number of nodes browsed than depth of search, and in widely connected environments the number of nodes even in short paths can be huge.

V. Summary and future work

We have developed a P2P communication system that integrates security into design. Its key advantages are following

- Although the system relies on a centralized authority to issue peer identities, its use afterward is decentralized, e.g., enabling secure communication in ad-hoc mode away from Internet.
- Incoming calls are filtered according to user's preference that can set the limit on hop count in friends' contact lists.
- All peers are authenticated using Host Identity Protocol, that also provides IPsec traffic encryption.
- Peers can be located behind NATs, be mobile and multihomed.

The system is currently in pilot use by the members of Networking Research Group at HIIT. The current number of users is 20 and we plan to expand to a hundred of users to cover whole institution. With a Nokia's N810 Internet tablet, users are able to exchange video and voice calls over P2PSIP secured by HIP, as well as use the instant messaging service.

As the number of pilot users grow, practical evaluation of SPAM prevention becomes feasible. Users can configure their P2PSIP proxy to admit a call from a given number of hops from friends' contact list with a web-based interface. Jointly with other group members, we are conducting a usability study to clarify current user perception of threats and security mechanisms in P2P communication systems.

References

[1] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423 (Informational), May 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4423.txt

[2] A. Gurtov, *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*. Wiley and Sons, 2008.

[3] IETF P2PSIP working group, http://www.ietf.org/html.charters/p2psip-charter.html.

[4] A. Gurtov, D. Korzun, A. Lukyanenko, and P. Nikander, "Hi3: An efficient and secure networking architecture for mobile hosts," *Computer Communications*, vol. 31, pp. 2457–2467, Jun. 2008.

[5] A. Mislove, A. Post, P. Druschel, and K. Gummadi, "Ostra: Leveraging trust to thwart unwanted communication," in *Proceedings of the 5th USENIX symposium on networked design and implementation*, 2008.

[6] A. Khurri, E. Vorobyeva, and A. Gurtov, "Performance of host identity protocol on lightweight hardware," in *Proceedings of the ACM SIGCOMM Workshop on Mobility in the Evolving Internet Architcture MobiArch'07*. ACM, 2007, pp. 27–34.

[7] A.-L. Barabasi, *Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life*. Plume Books, April 2003.