MI: Cross-layer Malleable Identity

Soon Hin Khor
NICT Japan
nethsix@gmail.com

Akihiro Nakao
University of Tokyo
nakao@iii.u-tokyo.ac.jp

***Abstract*—Access to Internet services is granted based on application-layer user identities, which also offer accountability. The revered layered network model dictates a disparate network-layer identity scheme for systems. We challenge this religious layered model adherence by demonstrating the practical benefits derived from a cross-layer identity scheme. Instead of a rigid identity, our malleable identity (MI) scheme empowers a traffic originator to fine-tune, on a per-case basis if necessary, her 3rd-party issued identity attributes embedded in an identity voucher (IV). When tagged to traffic, IVs benefit users, the Internet and services. A user can (a) control her traffic identifiability, ranging from anonymous, pseudonymous to personally-identifiable through attributes fine-tuning and (b) enjoy Internet-wide Single-Sign On (SSO) to network-layer Internet resources and application-layer services through IV persistence, without privacy loss naturally associated with SSO. The Internet and services can prioritize traffic, using IV attributes, as defense against Denial-of-Capability (DoC), Distributed Denial-of-Service (DDoS) and Border Gateway Protocol (BGP) prefix hijack/route forgery. MI is protocol/architecture-agnostic, and backwards/forwards compatible.**

I. Introduction

Identification is used by sentinels to control access to resources and hold its bearer accountable for resource abuse. The OSI/TCPIP layered network model dictates that identification for users at the application-layer (appID, e.g., email ID) and systems at the network-layer (netID, e.g., IP) be distinct on the merit that concealing unnecessary layer-specific details simplifies each layer's implementation and enables their innovation to evolve independently. Unfortunately, the uneven hour-glass network model accelerates application-layer innovation that can be independently and flexibly implemented at any end-host by any party, while stunting network-layer evolution that relies on cumbersome unanimity for deployment over multi-party owned network components [19]. Expectedly, appID schemes have matured significantly being bolstered with well-run infrastructures to tackle security threats, in particular, identity minting and accountability (including spoofing), which are paramount to security threats filtering and act as a critical foundation that application-layer resources such as online banking is teneted on, while netID efforts to address similar security concerns have languished at redesign [5], [14], with no deployment in sight, leaving network-layer resources exposed to spoofing, DDoS, etc.

Instead of an arduous redesign, we argue to use IP or its future incarnation only for connectivity, but inject the mature appID into network-layer headers, which is accessible cross-layer. The former ensures backwards and forwards compatibility while the latter bestows accountability to IP and higher level protocols, e.g., BGP, without rework, or their future incarnations, without design considerations, through a mint-resistant and irrefutable identity managed by readily deployed infrastructures and processes. The clear connectivity/accountability separation enables various connectivity constraints (dynamic addressing, mobility, etc.) and middleboxes (Network Address Translator (NAT), proxies, etc.) to share or manipulate netIDs without fear of traffic losing their origin identities (§VI-E).

MI's benefits are three-fold: (1) a user has control over her traffic accountability and privacy; instead of a rigid identity fixed with user details, we extend existing appIDs to be malleable, i.e., an MI consists of one or more unforgeably signed IVs affixed to her traffic, each embedding only chosen attributes with varying accountability, attested by distinct issuers, (2) her MI is used by multi-layers/hops/connections for realizing Internet-wide "single-sign on" (SSO), and (3) Internet and services can prioritize traffic based on accountable IV attributes to defend against DoC, DDoS and BGP prefix hijack/route forgery.

II. Benefits

To demonstrate the benefits of a cross-layer MI, we walk-through a scenario; an online store is celebrating Singapore's National Day by offering a discount to each exercise mat purchase only if the shopper is a Singapore resident and she provides her fitness club membership number. A shopper requests, through logging-on, for a residency-proving attribute from the Singapore government portal, *singpass.gov.sg*, e.g., a pseudonym, which is a hash of her residency number, and a membership number attribute from her fitness club's web server. The two issuers—portal and web server, will embed the respective attribute into a digitally signed IV each, for use together as her MI. She affixes both to her online store destined traffic. It is important to note that the residency-proving attribute is not the residency number hash, but rather the portal's digital signing.

User Accountability and Privacy Control In the absence of the MI scheme, she would have had to scan both her residential and membership cards and submit copies of them to enjoy the discount, thus exposing more data than necessary. Instead, the portal-signed pseudonym and fitness club web server-signed membership number sufficiently grant her discounted purchase and enables the online store to build a loyalty program for her, yet not personally identity her without additional information, e.g., shipping address, or assistance, e.g., collusion with attribute issuers. The former can be obfuscated through proxy receivers while the latter is an inherent SSO issue that we tackle using untrackable SSO (§III).

SSO With a single login at each IV issuer, the resultant IVs form her reusable MI. We loosely term this as "SSO"; despite the occurrence of multiple logins for identity formation, it remains true to SSO's goal of identity reusability for multiple resource access. Internet routers grant her traffic passage to the online store service and the service grants her the discount based on the same identity, albeit through different attributes; Internet routers use the pseudonym for accountability assurance while the online store uses both for criteria matching.

Internet and Services Security Defense Internet routers and services can effectively filter her traffic if she becomes a threat, or fair-share resource utilization during DDoS, based on the portal pseudonym attribute. The government portal will not grant her another pseudonym nor can she spoof someone else's pseudonym, without that person's login credentials, thus enforcing identity mint-resistance and accountability, which prevents her from evading filters or gaining unfair amount of resource.

III. Design

Our design goals for a cross-layer malleable identity are:

Mint-resistant An attacker should not be able to mint identities arbitrarily thus subverting attempts to filter as well as gain an unfair amount of available resource or unfairly influence resource allocation decision, ala a Sybil attack [10].

Accountable All traffic must be accountable to its originator; accountability enables traceback, filtering and resource fair sharing.

Malleable A rigid identity has restricted use, e.g., IP serves connectivity well; tunneling, proxying, peering, etc., is possible. However, for IP to be accountable, it requires a disruptive redesign, possibly at the expense of connectivity flexibility. A malleable identity, on the other hand, can shed/overload identity attributes at will, to meet various uses.

Multi-hop SSO A single-sign on to acquire vouched identity attributes gains access to resource at all hops, i.e., routers, middle-boxes and servers, from source to destination.

Multi-layer SSO The same identity attributes examined by network-layer routers are available to middle-boxes and destination servers at the application-layer for access control.

Multi-connection SSO The identity attributes can persist over multiple connections if desired, e.g., a pseudonymous identity used for making a comment on a blog should be usable to make a forum post without additional login provided both the blog and forum permit pseudonymity.

Untrackable SSO In the walkthrough, it is obvious that resource sentinels (verifiers) presented with IVs to verify their authenticity and contents can collude with their issuers to expose the bearer's true identity, which is an SSO plague that we want to overcome.

Simultaneous Multi-identity A user can acquire multiple identities, each with different vouched attributes, by logging in to multiple 3rd party issuers to acquire those attributes, and assign or switch her application's identity at will.

IV. Architecture

We achieve mint-resistant, accountable, and malleable identity, and multi-hop/layer/connection SSO through:

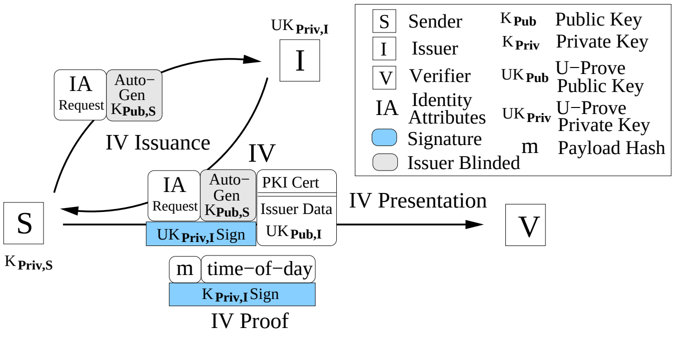

Fig. 1. In U-Prove, the sender public-private key pair is generated during IV issuance with the issuer blinded from it. The sender can selectively divulge a subset of her issuer attested identity attributes to a verifier for privacy control during the IV presentation.

AppID Scheme Adoption To combat bots minting appIDs or reusing stolen appIDs, which undermines accountability, CAPTCHAs [20] and user registration verification processes have been employed to protect self-service user registration, i.e., appID minting, while login credentials that can be fortified with two-factor authentication (2FA), defends against stolen appIDs. Both distinguish bots by exploiting a human's unique cognitive ability or her personal possession, e.g., email account, mobile phone or 2FA token. On the other hand, existing netID redesign proposals cannot fully address minting [5] or they rely on cumbersome mechanisms that force a user to relearn about identity concepts and user interfaces (UI), which hinders adoption, e.g., [14] employs Public Key Infrastructure (PKI) where a user's system identity manifests as a certificate. Conversely, adopting existing appID schemes for cross-layer identity enables the reuse of mature technology and established identity management infrastructures that users have become accustomed to, which fast-tracks netID mint-resistance and accountability.

IV An IV embeds attributes that reveal selected traffic originator information attested by a single 3rd party issuer. The attributes and issuer trustworthiness determine its mint-resistance and accountability level, e.g., an email provider issued IV attesting her email attribute has poorer levels of both compared to a government portal issued IV attesting her residency number pseudonym attribute since email providers do not perform user validation and do not restrict each person to a single identity instance.

MI A user may group her IVs into different combinations to form multiple MIs, each with a unique attribute set, which she can assign to different applications running on her system. Forging multiple MIs does not constitute arbitrary identity minting because each MI merely contains a different subset of her entire IV attribute set in order to fine-tune each identity to expose minimal user identification required for resource access.

U-Prove U-Prove technology [7] is chosen for IV (synonymous to U-Prove token) creation because U-Prove tokens: (1) are truly untraceable even when issuers-verifiers collude, which is key to untrackable SSO, (2) not transferable, and (3) not replayable.

An issuer signs requester (or sender, short for traffic originator) attributes that she can vouch using her U-Prove private key and the signature is verifiable using the U-Prove public key from the PKI certificate embedded in the IV (Fig. 1). Although during issuance the issuer has no knowledge of where an IV will be used, i.e., untrackable, colluding issuers-verifiers can correlate any one of the three fields (sender identity attributes, sender public key or issuer U-Prove signature on sender identity attributes and public key) of issued and presented IVs to track an IV usage. U-Prove's novelty stems from the non-visibility of signatures generated and the auto-generation of a sender public-private key pair, which is blinded from the issuer, during IV issuance, making sender identity attributes the only trackable field, which a sender has full control of, thus can easily thwart by embedding only pseudonymous or anonymous identity attributes (1).

During an IV presentation (Fig. 1), a sender produces an "IV proof" by signing the time-of-day and the packet content hash, using her private key, which is verifiable with the corresponding public key in the IV. Successful proof presentation, which is an indication of private key possession, is not possible if an IV-proof pair is stolen and affixed to packets with dissimilar contents (2). However, the entire packet-IV-proof is actually replayable (3) within a short period of time prior to the IV proof expiring, i.e., a configurable time lapse after the time-of-day encrypted within, which we address in §VI-C. The reusability of an IV and its persistence over communication enable multi-layer/hop/connection SSO.

Accountability Lever The accountability lever provides a UI to define multiple MIs and per-application/destination identity assignments—which identity is utilized for each application-/destination combination, e.g., assigning an identity with email attribute IV to browser-forum, browser-blog interaction while an identity with government portal pseudonym IV to browser-online store communication.

V. Assumptions

Secure Autonomous System (AS) Border Routers AS border routers are critical Internet components that receive meticulous attention from owners to ensure their security, robustness and correct operation. We assume that they can be trusted to transfer IV attributes to packet headers and signing them faithfully, as required by LS signature scheme, described next (§VI-A), which is necessary to achieve high-speed per-packet signature generation and verification,

Root Certificate Authority (CA) List An issuer needs a U-Prove private key to sign sender attributes to create unforgeable IVs. Although the corresponding U-Prove public key used for IV verification is packaged into the IV, verifiers need to ascertain that the public key indeed belongs to the said issuer by ensuring that the PKI certificate embedding the public key has been attested by a CA traceable to a trusted root CA; this merely mandates that verifiers keep an updated list of root CAs, which is what web browsers are currently doing. Users are not exposed to the PKI complexity.

Trust-reliant Internet Security With IV verification and root CA attestation, one can conclusively determine that an issuer vouched for some sender's attributes. However, judgment of an issuer's trustworthiness not to lie about those attributes must be aided by previous interaction, business relationships, or reputation systems.

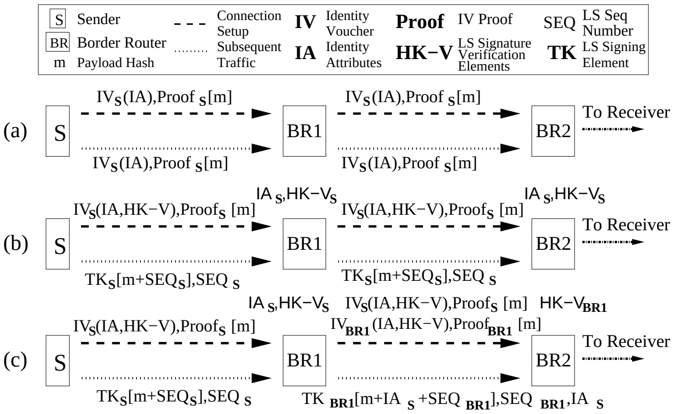

Fig. 2. '()" indicates contains and "[]" input. To reduce diagram clutter, public key in IV and time-of-day in proofs have been omitted. (a) Traffic is highly accountable but the IV proof generation at S and verification at BRs are resource costly. (b) Use LS signature to replace costly IV computations after connection setup. (c) Introduce identity NATing where a BR's LS signature represents all senders under its aegis to reduce the number of HK-V's downstream routers need to keep. A sender's IA is transferred onto NATed packet headers by the sender BR to retain sender identity.

VI. Discussion

A. High Throughput and Resource Consumption Scalability

The naive architecture described thus far meets our accountability and SSO goals but costly and time-consuming per-packet IV proof generation at senders and verification at forwarders/receivers (F/R) will hinder scaling to Gbps speed (Fig. 2a). We overcome it by introducing:

Lightweight Signatures (LS) We replace the IV proof with our LS scheme based on [14] after connection setup (Fig. 2b). In LS, a public hash key (HK) and a signature verifying number (V) are verification components used by F/Rs while the corresponding trapdoor key (TK) is the signing component possessed only by the sender (details in [14]). The key feature is signature generation and verification are fast, involving only one-way Message Authentication Code (MAC) manipulations but at the expense of signature degradation in a shorter time period, resulting in HK-V needing updates securely every few days; accepting HK-V from an impostor leads to possible signature forgery and accountability degradation. In our scheme, HK-V is updated as a sender IV attribute vouched by an issuer who has validated the sender as elaborated below. Without loss of generality, we describe LS using a scenario where a sender's MI attributes is comprised of a single IV, so the terms identity and IV can be used interchangeably but barring the number of signature/IV proof generation and verification, the entire process remains unchanged when an MI comprises multiple IVs.

During connection setup, a sender requests the issuer to vouch her desired attributes and digitally signs them including her arbitrarily selected HK-V, creating an IV bonding sender IV attributes and HK-V; subsequent IV-less packets bearing the sender's TK generated signature verifiable by this HK-V implies same sender identity. She also generates an IV proof and affixes both IV and proof onto the setup packet. This packet will travel from sender through forwarders to receiver once so that F/Rs can inspect the IV-proof for themselves and store the associated HK-V to verify subsequent packets.

A sender-unique sequence number (SEQ) is affixed each LS packet to prevent replayability (§VI-C).

Identity NATing Tracking the HK-V for every possible sender identity, which each sender can possess multiples of, at each forwarder will not scale, thus, an AS border router (BR) is expected to "NAT" the senders within so that other downstream AS BRs only need to track the NAT router's HK-V instead (Fig. 2c). Although we only describe identity NATing at AS BRs, it can be extended to stub routers and transit AS BRs, with each additional NAT layer further easing resource requirements at the expense of exposing a larger attack surface area.

To distinguish between packets exiting a NATing BR, each packet has to retain its sender IV attributes all the way to the receiver by trusting the BR to transfer the IV attributes onto a packet header field and signing it with its TK so that downstream F/Rs can verify and trust the integrity of the transferred attributes. For each connection setup packet, the sender AS BR verifies its IV, extracts and stores the IV attributes against the sender HK-V for non-setup packet use later, appends into the header an IV vouching for its BR HK-V and the BR IV proof based on the time-of-day and packet content hash thus claiming accountability for this packet. F/Rs can firstly inspect the original sender IV attributes and packet content authenticity but instead of the sender HK-V, they store the BR HK-V once the BR's IV proof is verified. For subsequent packets, a sender, with its TK produces a sender signature, in place of time-consuming IV proof generation, which upon correct verification at the sender AS BR, the BR inserts the IV attributes stored against this sender HK-V during connection setup and replaces the sender SEQ with its own before signing using her BR TK over the packet content hash, including the inserted IV attributes and new SEQ.

For every AS BR to posses each other's HK-V, all AS representative systems, e.g., each AS's designated PC, initially exchange all their BR IVs acquired from their own AS issuers that vouch for each's HK-V. Subsequent updates of HK-V, which is necessary as the TK secrecy erodes quickly over time, are exchanged with messages "signed" by each BR's previous TK, prior expiry. Each representative system is responsible for making all exchanged BR HK-Vs available to its AS's BRs.

B. Security Defense

1) DDoS: For DDoS defense, we introduce:

IV-based Prioritization and Rate-limit Since accountable packets have unique unforgeable pseudonyms/identifiers that provide a basis for fair-sharing network bandwidth, traffic regulation policies should favor them using a two-level prioritization scheme based on (1) IV accountability level (Table I) and (2) IV issuer trustworthiness. Packets with the same accountability level are segregated based on their IV issuer trustworthiness, which is judged from their mint-resistance and accountability enforcement. In addition, rate-limiting offers protection against a bandwidth-hungry user or a bot-infected system with a high accountability identity. Poor accountability DDoS packets will have low priority thus unable to disrupt more accountable legitimate traffic while high accountability DDoS packets that are detectable can be accurately trace-backed and filtered, with undetectable ones are rate-limited based on their unique accountable attributes to enforce fair-sharing.

Accountability Level	IV Attribute(s)	Example
IV-less	None	Legacy packets
Group Pseudonym	Attributes of a group	Attendee of ICC 2011
Temporal Pseudonym	Attribute pseudonym that varies at each IV request	Session ID used to temporarily differentiate online store guests until they complete purchase
Persistent Pseudonym	Attribute pseudonym that persists over IV requests	Persistent nicknames used for associating virtual resources, e.g., points for answering forum posts
Personally Identifiable Information	Attribute that uniquely identifies a user	Residency Number

TABLE I
ACCOUNTABILITY LEVELS IN INCREASING ORDER FROM TOP TO BOTTOM.

2) DoC: For DoC defense, we introduce:

Localized Issuers The IV acquirement process (termed as a capability in computer science literature) can be thwarted by an attacker's indistinguishable capability request flood—Denial-of-Capability (DoC) [16]. Replicating issuer systems or locating their proxies, which tunnel IV requests to remote issuer systems, close to senders, ideally in their Internet Service Provider (ISP) networks, increases availability and facilitates attack filtering; only IV requests from within an ISP are served thus reducing the attacks to bots within, which is under the ISP's control to eradicate. This exerts economic pressure on ISPs; the inability to attain an IV leading to a customer experiencing poor connectivity, reflects an ISP's inability to keep its user base bot-free. Issuer systems or their proxies can utilize technologies such as virtualization to share infrastructure at distributed locations to reduce cost.

3) BGP Prefix Hijacking: BGP prefix hijacking occurs because the mechanism to verify that a prefix announcement originated from the legit prefix owner is missing. SBGP [11] is cumbersome because it requires two distinct steps to verify the tripartite relationship of prefix-owner-signature; confirm that the prefix is owned by a certain AS from the prefix allocator database, and the public key used to verify the announcement signature is indeed owned by that AS through ensuring the public key-owner vouching certificate's chain of trust leads to a trusted root CA. With MI, BGP is naturally secure in its current manifestation. We reduce the laborious prefix-owner database cross-checking step to a mere IV verification; the prefix owner is responsible for acquiring an IV attesting her prefix ownership from her prefix allocator, and affixing it to her announcement. Upon IV verification with the U-Prove public key from the PKI certificate embedded in the IV, a BGP router just needs to ensure that the certificate vouches a prefix allocator as the public key owner and its chain of trust is rooted to a CA in her local trusted root CA list.

4) BGP Route Forgery: We prevent route forgery using the same mechanism as SBGP; each BGP router appends the neighbor AS number to whom it will relay a prefix announcement, to the announcement's next BGP hop list and signs it, to prevent tampering of the list used to build BGP routes. The difference is instead of using expensive public key computations, we can leverage on the ease of secure dissemination of LS elements, TK and HK-V, to all AS BGP routers, for lightweight signing and verification respectively.

C. Inherent Security Concerns

Replayability Packet replayability may result in F/Rs wrongly forwarding/accepting a packet when they should not, resulting in DDoS or corrupted receiver state. Connection setup packets can be strictly rate-limited using uniquely accountable IVs (§VI-B1) since initiating many connections to a single destination is definitely an undesirable anomaly. A non-setup LS packet replayability is restricted to locations where F/Rs expect them thus possessing necessary components, i.e., HK-V, for signature verification; LS packets captured within an AS cannot be replayed outside that AS. Moreover, with SEQ tracking at AS BRs, replayed LS packets will be dropped and cannot deluge neighboring ASes. Receivers keeping track of SEQs can prevent re-processing a replayed packet thus averting state corruption.

Mint-resistance and Untrackable Conflict If an issuer generates a unique pseudonym for a requester, it is trackable through verifier-issuer collusion. If a requester is permitted to arbitrarily select a unique pseudonym that the issuer is blind to at IV generation, the requester attains ability to mint arbitrary identities. Preserving both mint-resistance and untrackability is thorny but possible with U-Prove tokens; an issuer will blind sign anything by the sender, e.g., unique pseudonym, but only once until IV expiry, to create an IV with *all* requested attributes in tow. U-Prove's unique property of enabling a sender to reveal only selected attributes during IV presentation ensures that she does not lose the control of her privacy.

D. Issuer Incentive

A government portal has little incentive to offer unique pseudonym attribute IVs that users may acquire for the portal-unrelated purposes, e.g., affixing the IV to their traffic to increase accountability and acquire priority forwarding from ISPs or utilizing the unique pseudonymity at an online shop for privacy protection. ISPs offering free hosting for the portal's issuer systems is a possible carrot; the portal acquires high redundancy in return for IVs that bestow accountability on the ISP traffic. Another possibility is each ISP setup an issuer system that their users can acquire IVs attesting their ISP subscription number, which offers accountability.

E. Peering Through the Shroud

Multi-user systems, dynamic addressing, mobility, and middle boxes (NAT, proxies, etc.) multiplexes users onto a system netID to enhance connectivity but degenerates accountability and tints Internet measurements [8]. In MI, connectivity and accountability are clearly delineated; resource access and measurements are made based on persistent 3rd-party vouched accountable IV attributes that middle-boxes cannot alter/override while netIDs can be manipulated as necessary for connectivity purposes. For example, middle-boxes that users exploit to conceal their true nature, such as, falsifying location information through proxies to access country-restricted content, can be averted through vouched IV attributes.

F. Resource Consideration

We consider MI's resource consumption in terms of CPU, memory, network resource, and packet size.

CPU CPU-expensive IV proof generation and verification is done only once in connection setup. Established connection packets use lightweight MAC-based LS scheme for those functions, whose high-speed feasibility has been studied [14].

Memory Memory incurred to keep a Bloom filter for packet replay detection is not necessary for packets with IVs since ensuring packet freshness by checking the time-of-day in its IV proof and rate-limiting based on the IVs will suffice.

LS packet's limited replayability location makes having a global view of all packets unnecessary. Thus, each forwarder keeps only a local copy of observed SEQs. [14] has shown that with a 32MB RAM Bloom filter, a forwarder can track 1s of traffic with 32-bit SEQs in a 2Gbps link with negligible probability of wrongly identifying a replayed packet.

Currently, TCP already tracks sequence numbers demonstrating that SEQ tracking at a receiver to avoid re-processing a replayed packet is not a show-stopper.

Network Resource Message exchanges are required for a signer to keep others updated on her new HK-V, which is necessary to alleviate signature degradation. A sender hardly emits beyond 50,000 packets/sec [5] thus a 32-bit long SEQ can introduce sufficient entropy to prolong her HK-V for $2^{32}/(3600*24) \approx 1$ day prior a required update. A BR that NATs sender packets will exhaust her SEQs faster but message exchanges required for HK-V updates are much fewer than existing routing updates that a BR currently handles.

Packet Bloat The connection setup packet size bloat caused by embedding a single IV-proof is at least 1205 bits, subject to the sender attributes' size. For a single-IV MI, which is the norm, the packet bloat is comparable to other accountability proposals; [5] requires at least 600 bits with increments in multiples of 160 bits if an AS is subdivided for administrative purposes. For a multi-IV MI, a designated issuer can be trusted to merge all the IV attributes and re-issue it as a single IV. For non-setup LS packets, the size is at least 256 bits, subject to sender attributes' size.

G. Deployability

Protocol/Architecture-agnostic MI does not modify any packet fields but appends some of its own; it can be integrated into any protocol that supports additional arbitrary fields.

Backwards-compatibility An MI-unaware sender will not affix IV on her packets, thus they will be forwarded on a best-effort basis like in the current Internet. An MI-unaware F/R can handle packets by ignoring affixed IV.

Incremental Deployment Benefits If a stub AS (one that does not transit traffic) deploys MI, its senders' packets can enjoy priority handling by any MI-compliant F/R along an end-to-end-path, the AS's prefix can be protected from BGP prefix hijacking, its receivers and the AS itself can prioritize packets to mitigate DDoS. Although network externality exists, i.e., without sufficient adopters, benefits may not be compelling, the critical participation rate required is less foreboding; the above benefits are reliant only on stub ASes' adoption. Adoption at transit ASes is nonetheless helpful in optimizing DDoS defense by dropping attack packets sooner.

VII. Related Work

Internet Accountability The importance of Internet accountability has spawned much research [14], [5], [13], [21]. [5] is a clean-slate design that requires an overhaul starting from applications, hosts, all the way to routers. [13] can provide AS granular accountability where each AS vouches for its packets that others can verify using pre-exchanged symmetric keys. Only when combined with [21], it offers BGP attack protection that relies on DNSSEC deployment becoming mainstream and multi-party to diligently co-operate to preserve the integrity of the reverse DNS entry-AS public key certificate (prefix-owner-signature) associations. However, [21] requires AS renaming, which may face resistance. None of the proposals provide SSO. In MI, any authentication system can provide an identity as long as the vouched identity attributes are forged into an IV using a development library that we intend to provide. Accountability is voluntary; a user can balance between her accountability and privacy needs, with the former granting her traffic more privileges and if consented, is traceable at user granularity. Most significantly, by being cross-layer, new and existing protocols, e.g., BGP, can access MI to inherit its accountability with no rework or design considerations.

Network-layer Tokens Research embedding network-layer capability tokens into packets for Internet traffic control is not new. They differ on the embedded information, purpose and technicalities that make them unforgeable and their authenticity verifiable. A network capability token [6], [22] enables a receiver to control traffic reception. A proof-of-work (PoW) token [16], [12], [9] enables a sender to compete for overwhelmed resources. An ICING token [17] signals ISPs' pre-agreed packet itinerary and enforces it. A Platypus token [18] enables the transfer of network usage rights to others. IV does not dictate the embedded information but only outlines a framework for creating unforgeable, verifiable yet untrackable tokens. Its generality enables it to emulate all token schemes above as well as others not mentioned here.

SSO SSO is commonly implemented using tokens or on-demand identity verification. In the former (MI, Kerberos [15]), a user that authenticates successfully to an identity provider is issued an unforgeable token that she can present to verifiers. In the latter, (OpenID [3], Shibboleth [4]), prior resource access, a verifier will request an on-demand user verification from her identity provider. Unlike tokens, which are reusable till expiry without identity provider interaction, on-demand identity verification systems have to be redundant to handle continuous requests from verifiers. Only IV tokens support multi-layer/hop SSO naturally due to their persistence at the network-layer, which is accessible cross-layer and verifiable by all. A Kerberos token is encrypted with its destination secret key at application-layer, restricting its verifiability to that end-point at that layer, negating multi-layer/hop SSO support. The most glaring deficiency, however, is that with the exception of MI, token issuers and on-demand identity verification systems can observe a logged-in user's access trails.

Malleable Identity Microsoft's CardSpace [2] and Higgins Framework [1] enable a user to self-create and manage multiple identities, which offers malleability but is restricted to the application-layer for online identity protection, while MI is a cross-layer 3rd-party attested identity scheme that extends into the network-layer for traffic protection.

VIII. Conclusion

This paper presents a non-conformist way to achieve network-layer accountability; instead of striving to make IP or its future incarnation accountable, we persist with IP for connectivity but infuse application-layer malleable identity (MI), an extension of existing application-layer identities where a user has control over identity attributes she wish to expose to fulfill resource access criteria, into network-layer headers as a cross-layer accountable identifier. The rationale is existing application-layer user identities are already mint-resistant and accountable, complemented with well-run user-friendly infrastructures and processes that we can adopt to fast-track network-layer accountability that researchers are grappling with. MI persistence enables users to enjoy a "single-sign on" to Internet-wide multi-hop/layer/connection resources while its accountability empowers the Internet and services to defend against DDoS, DoC, and BGP prefix hijacking/route forgery. Any existing or new protocol can inherit MI's accountability without rework or design considerations due to its cross-layer accessibility ensuring any practical deployment experience in the current Internet can be migrated to the future one.

References

[1] Higgins Framework. www.eclipse.org/higgins/.

[2] Microsoft CardSpace. http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx.

[3] OpenID Foundation. http://openid.net.

[4] Shibboleth: A Project of Internet2 Middleware Initiative. http://shibboleth.internet2.edu/.

[5] D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker. Accountable Internet Protocol. In *SIGCOMM*, 2008.

[6] T. Anderson, T. Roscoe, and D. Wetherall. Preventing Internet Denial-of-Service with Capabilities. In *Hotnets*, 2002.

[7] S. Brands. Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy. *MIT Press*, 2000.

[8] M. Casado and M. J. Freedman. Peering Through the Shroud: The Effect of Edge Opacity on IP-Based Client Identification. In *NSDI*, 2007.

[9] C. Dixon, T. Anderson, and A. Krishnamurthy. Phalanx: Withstanding Multimillion-Node Botnets. In *NSDI*, 2008.

[10] J. R. Douceur. The Sybil Attack. In *IPTPS*, 2001.

[11] S. Kent, C. Lynn, and K. Seo. Secure Border Gateway Protocol (SBGP). In *IEEE Jour. Comm.*, 2000.

[12] S. H. Khor and A. Nakao. sPoW: On-Demand Cloud-Based eDDoS Mitigation Mechanism. In *HotDep*, 2009.

[13] X. Liu, A. Li, X. Yang, and D. Wetherall. Passport: Secure and Adoptable Source Authentication. In *NSDI*, 2008.

[14] J. Mirkovic and P. Reiher. Building Accountability into the Future Internet. In *NPSEC*, 2008.

[15] C. Neuman, T. Yu, S. Hartman, and K. Raeburn. The Kerberos Network Authentication Service (V5). *RFC4120*, 2005. http://www.ietf.org/rfc/rfc4120.txt.

[16] B. Parno, D. Wendlandt, E. Shi, A. Perrig, B. Maggs, and Y.-C. Hu. Portcullis: Protecting Connection Setup from Denial-of-Capability Attacks. *SIGCOMM*, 2007.

[17] A. Seehra, J. Naous, M. Wafish, D. Mazieres, A. Nicolosi, and S. Shenker. A Policy Framework for the Future Internet. In *Hotnets*, 2009.

[18] A. Snoeren and B. Raghavan. Decoupling Mechanism from Policy in Internet Routing. In *Hotnets*, 2003.

[19] J. Turner. Virtualizing the Net - a Strategy for Enabling Network Innovation. In *IEEE Symp. on High Perf. Interconn.*, 2004.

[20] L. von Ahm, M. Blum, N. Hooper, and J. Langford. CAPTCHAS: Using Hard AI Problems for Security. In *EuroCrypt*, 2004.

[21] X. Yang and X. Liu. Internet Protocol Made Accountable. In *Hotnets*, 2009.

[22] X. Yang, D. Wetherall, and T. Anderson. A DoS-limiting Network Architecture. In *SIGCOMM*, 2005.