A Design of User-Centric Intranet

Xiaoliang Zhao, David Kao
Time Warner Cable Inc.
Herndon, VA, USA
{leon.zhao, david.kao}@twcable.com

Jilong Wang, Xing Li
Tsinghua University
Beijing, P. R. China
{wjl, xing}@cernet.edu.cn

Dan Massey
Computer Science Department
Colorado State University
Fort Collins, CO, USA
massey@cs.colostate.edu

Abstract— **Many intranets today are built on top of TCP/IP network architecture, which was originally designed for data communication between computers. Human users have been little considered by the architecture. In this paper, however, we argue a user-centric instead of computer-centric architecture provides better management, usability, accountability and more for intranets. As a first step towards such architecture, we focus on one fundamental problem: the representation and implementation of user identity. We propose a design based on IPv6 and a special edge control device. Then we discuss its implications to security, privacy, network applications and operations.[1]**

Keywords- user-centric network, security, privacy, accountability

I. INTRODUCTION

Many intranets, such as university campus networks and enterprise networks are built on top of TCP/IP network architecture. When TCP/IP was originally designed more than thirty years ago [1, 2], the goal was to define a language so computers can understand and communicate with each other. As a result, such network architecture enables a computer-centric communication model, and the human users have been little considered. Separation of the network and its users has its advantages, such as resources can be easily shared by different users, network can be comparatively easy to manage without extra user management overhead, and user privacy is better protected, etc.. However, it also brings some issues. For example, since users are not recognized by the network at all, it is very difficult to trace a network security breach back to the user who is responsible for. As noted in [4], lack of user accountability at network level creates a fundamental challenge to network security. Another example is more user experience related. Nowadays, it is not uncommon for a user to maintain multiple user accounts to different network applications. Even inside a company intranet, which is usually tightly controlled by a single administrative unit, an employee may still maintain multiple accounts to access different computer systems because of legacy issues or organizational issues[2]. Most users found it inconvenient and it may weaken the overall security as well [8]. Many organizations have adopted Single Sign-On (SSO) approach to work around the issue, but the fundamental limitation remains in the architecture itself.

These are just couple of examples motivating us to re-think the relationship between a network and its users. What if a network be designed and built around users instead of computers? Isn’t the purpose of a network to serve its users, hopefully in a convenient and secure manner? In light of such thinking, we believe a network built around its users will find its own values. In this paper, we explore the idea of User-Centric Intranet (UCI). In an UCI, each user can be uniquely identified at network layer so that network becomes user-aware. We argue that in an intranet environment, UCI provides better network security via user accountability and the integration of network security policy with user account management. It may also help build user-aware network applications to offer better user experiences. Such arguments will be presented in section II in more detail. In section III, we demonstrate the feasibility of UCI concept by presenting a high-level design based on IPv6 addressing schema and Network Access Device (NAD). Section IV briefly discusses some potential issues and we review related works in section V.

II. USER-CENTRIC INTRANET

User-Centric Intranet (UCI) is defined by its capability to uniquely identify a user at network layer in an intranet environment. But why one may ever need UCI? We believe it is because Intranet has its unique characteristics than the Internet. First, most intranets are built for business purpose where security and efficiency takes higher priority than other requirements. For example, it is not uncommon for a company to audit its employee’s network activity to ensure the overall network security. Second, an intranet often is guided by its organization’s policy and enforced by a centralized and

[1] The majority of this work was done when Xiaoliang Zhao was with Tsinghua University.

[2] One author himself maintained more than fifteen different active accounts when he worked for a large international company.

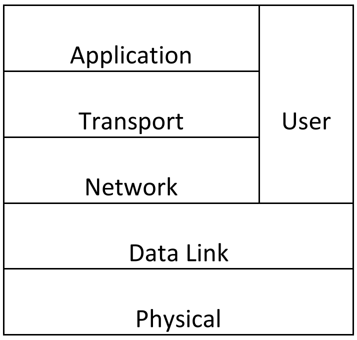

Fig. 1: UCI architecture

dedicated effort such as IT department. On the contrary, the Internet has no such centralized governing entity. With such observations in mind, we believe UCI may serve better its business purpose. Below are some high-level thinking on what benefits UCI concept may bring to the intranets.

A. *Enhanced overall network security via Accountability*

Network security is one of main concerns for years. We share the same belief stated in [4] that many network vulnerabilities today are due to lack of accountability at network level. UCI adds such accountability to complements the existing security systems such as firewall, IDS, AAA systems, and helps thwart the attackers, especially insiders who are difficult to be detected by traditional means. As a matter of fact, insiders are considered to be most costly to many organizations [16].

B. *Simplified network management*

Network management can be a real challenge, especially in a large intranet with geographically located offices and changing working forces such as contractors and outsourcing staffs. Taking firewall management as an example, in most cases, network security policies are implemented by firewall rules. However, firewall rules are often based on IP addresses or port numbers, but policies are often designed and expressed based on users or their roles, such as “a guest cannot access my intranet”. The mismatch between policy expression and firewall rules creates a non-trivial work to maintain a mapping between two of them. In a changing environment, such mapping tends to be dynamic and can potentially weaken the overall security by mistakes or unintentional negligence. To address such challenge, some commercial products integrate user identities to network address assignments, firewalls, LAN switches or other security devices [5,7]. UCI directly integrates user identities, possibly along with role information [17], into network layer. Firewall management then can be greatly simplified because security policies and their firewall implementation can refer to same objects without extra mapping or translation.

C. *Unified user identity across different layers*

Large companies often have many different internal computer systems which use different user authentication mechanisms. It sometimes is a non-trivial work for an employee to manage all his/her credentials. A poor username and password management in such case may cause big security breaches [8]. In UCI, it is possible for a user to have a single identity all the way up to the application layer. So a user may only need maintain one user ID and its associated credential. Once the user is authenticated by the network layer, the same user may not need to authenticate himself or herself to different applications again, which provides opportunities to improve the work productivity.

4	4	8	16	32
Type	Control	Interface index	User group	User ID

Fig. 2: UCI user addressing scheme

III. An IPv6 based design

The first question one may ask is if UCI idea even can be possibly realized in the real world. In this section, we present our design of an IPv6 based UCI network, named Tsinghua User-Centric Accountable Network (TUCAN). Tsinghua University campus network (TUNet) serves more than 30,000 users. Such large user base and the variety of applications running on top of TUNet create an ideal setting for the experiment to obtain meaningful results. Through TUCAN, we hope to demonstrate the possibility to build a practical UCI network.

Only very recently, the emerging IPv4 to IPv6 transition provides a viable path as well as an early opportunity to realize UCI idea. Leveraging IPv6 technology makes our work different from many others. Such approach may also benefit both UCI and IPv6 development. On the one hand, IPv6 huge address space and its readily available software and hardware platform make UCI more practical. On the other hand, UCI provides opportunities for innovative applications and services which may help boost IPv6 deployment.

The key issues need to be addressed by TUCAN design include the definition of user, the representation of user identity, how to integrate user as a new layer with TCP/IP architecture and how user layer interacts with other layers. TUCAN design made the following decisions.

- A user in TUCAN network corresponds to a real person, such as a student or a faculty member who is identifiable in the real world with a unique identification number, such as a student ID number. The same user identification number or a derived form may be used in TUCAN network to uniquely identify a user. We assume there are no two different numbers identifying the same user. In addition, we assume a user database which includes all user information, including each user’s identification number, his/her role or group, and other personal information which may be relevant to network access control and network management. Such user database should be securely guarded and may only connect to a private LAN for internal use only.
- TUCAN architecture is illustrated in Fig. 1. A new layer, user layer, is introduced and inserted into the architecture vertically in a cross-layer fashion. User layer implements

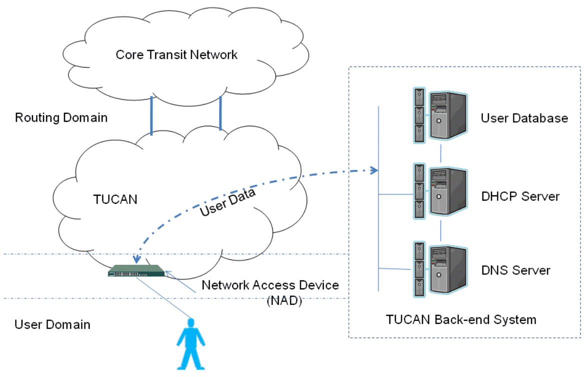

Fig. 3: TUCAN Design

UCI definition, i.e., to uniquely identify a user at network level. It also provides a simple service to other layers such as providing user identity information to other layers. A cross-layer design helps eliminate communication overhead between different layers.

We describe more technical details of TUCAN design in the following subsections.

A. *Addressing*

The very first step is to determine how to name or address a user in the network level. We take the advantage of huge address space IPv6 provides and propose to use the first 64 bits as network address for routing purpose, and last 64 bits to store user identification number and other related information. Such addressing scheme is very similar to [9], but we use the last 64 bits in a completely different way.

Information put in the last 64 bits will have great impact on the network properties of TUCAN. It is quite critical to determine what information should be put there and in which structure. Our design, as illustrated in Fig. 2, reflects our understanding on network operation and network management requirements. First, a type field provides extensibility for future different addressing specifications. In particular, type 1 refers to our design. The control field stores control bits, such as the user status bits (a user is active or not) and the global or local significance of User ID field. We recognize the fact that more and more users own multiple devices to connect to the network, and the Interface Index field is to differentiate which device a user is using. User Group field is for network management purpose since group-based policy is much easier to maintain than individual user-based policies [17]. In TUCAN, user ID field takes 32 bits. To some extent, it may provide certain backward compatibility to transport and application layer, which do not need to modify its software data structure as if User ID were a regular IPv4 address.

We assume there is a separate IPv6 address space for TUCAN, so networking devices can interpret TUCAN IPv6 addresses differently. Non-TUCAN IPv6 addresses will be treated in the traditional way without user ID extraction and interpretation. TUCAN address space can be obtained through address allocation from Regional Internet Registry such as APNIC. Or alternatively, special marks can be put in the rightmost part of first 64 bits, if those bits are not used for routing purpose, to indicate it is a TUCAN address.

B. *Routing*

By splitting an IPv6 address into two parts, TUCAN design explicitly divide the network into two domains connected by Network Access Devices (NAD), as illustrated in Fig. 3. The network devices such as switches and routers in the routing domain forwards the data packets as usual based on the first 64 bits of the IPv6 address. The data packet is eventually delivered to the destination edge device where the receiving user will be located and data will be forwarded without further routing. By clearly separating routing domain from user domain, the routing domain is left untouched, which helps reduce the deployment cost.

C. *User Network Access and Security*

In TUCAN, all users gain the network access through authentication process at the edge of the network. It is different from traditional TCP/IP networks as the authentication becomes mandate process in TUCAN. It seems we are falling back to old-fashioned dial-up way, but it is the essential step for TUCAN to be able to identify users[3]. Network Access Devices (NAD) participate the authentication process and enforce the results. More specifically, a user gains the network access through the following steps:

1. User A first gets a regular IPv6 address through usual means to communicate with TUCAN back-end systems.

2. A sends out a DHCP request to the DHCP server, along with his/her credentials and other network access related information via a secure channel.

3. DHCP server queries the user database, *e.g.*, a RADIUS server, to authenticate A. If passed, DHCP server sends back an IPv6 address, *P*, with information properly populated into each field, including network address, control bits, A's group, A's ID, etc..[4]

4. NAD sniffs DHCP traffic and upon receipt of DHCP reply, NAD records 1) A's MAC address through which DHCP request was sent, 2) *P*, 3) which physical port on NAD device DHCP traffic went through, and optionally 4) A's ID,. This record, referred as a *NAD binding*, will be stored in NAD memory and be used for network access control purpose.

One may notice that the role of DHCP server is slightly changed. It is not solely to assign network addresses, but assumes more user management responsibilities. In addition to carry assigned IPv6 addresses, DHCP traffic functions as signaling messages to inform NAD to open or deny network

[3] Correspondingly, user can log off from the network by sending an explicit logoff request.

[4] TUCAN allows DHCP server to assign a user with different IPv6 addresses depending on user's explicit requests and the network policy. For example, a user may explicit require an anonymous IPv6 address to protect his/her privacy and the DHCP server should honor such request if policy allows.

access for a particular user. Once a user passed the authenticated at the edge of the network, TUCAN allows the user to access different applications without authenticating the same user again. It is similar to the common practices that when a user successfully logs in to an operating system, normally it does not require the user to log in to each individual application again. TUCAN simply extends the same practice to the network level. For example, once a student login to TUCAN, he/she is able to browse his/her saved searching records from library servers or his/her own class materials from department servers, no need to log in again as the servers will recognize the student's identity from source IPv6 address.

D. *Security Analysis*

Because DHCP server assigns IPv6 addresses based on static information, it means the same user will get same IPv6 address most of the time. If an attacker is able to sniff DHCP traffic or through social engineering, it seems possible for the adversary to statically configure an IPv6 address to impersonate others. However, the network access is enforced by NAD bindings which checks MAC and IP address as well as which physical port data packets coming in. In another word, the attacker has to connect to the same NAD port with masqueraded MAC address as the impersonated user, which can be quite difficult in most cases and also can be detected relatively easily, for example, by user's device to detect duplicate MAC address on the LAN.

However, in a wireless network, it becomes more challenging because users are not connecting to physical ports any more. Therefore physical ports cannot be used as part of NAD binding. One way to address this issue is to use the security channel between user's device and the wireless Access Point (AP) as part of binding. More precisely, a dynamic session key will be established between the user's device and AP after the authentication process. The session key not only provides a secure communication channel but also acts as a virtual port to NAD. An adversary now need to masquerade MAC and IPv6 address, but also to break the session key in order to impersonate. Other approaches like secure heart-beat protocols may also help, *e.g.*, a keepalive message is periodically exchanged between user's device and NAD, which are encrypted by a shared key only known by the legitimate user. Such protocol certainly warrants further research. To further defend against identity theft attack, TUCAN also exploits the soft-state principle by deleting NAD bindings when a user is logged off from the network, or a failure occurred during secure heart-beat protocol, or simply a configured timer timed out.

NAD device is the security checking point for a user to enter TUCAN. Its security is critical to the overall network security. NAD devices should be managed only by the management network through a secure out-of-band channel. User's traffic and management traffic are separated both physically and in different address spaces to ensure no users can launch attacks, including DDoS attack, from user's address space. The same management network also manages other parts of UCI network infrastructure, including routers, switches and backend servers, in the similar manner. The management network itself should be secured via usual means such as jumping hosts, RADIUS servers, one-time password and so on.

E. *Direct Inter-User communication*

By adding a simple step in user authentication process, TUCAN may be able to enable direct inter-user communication, as if each user owned a "TUCAN phone number" and other users can call or communicate with him/her directly. Referring to the authentication process described in the previous section, after a user is authenticated, DHCP server can send a new DNS record to the DNS system, which adds a new AAAA record for user A, for example,

$$\text{A.tucan.tsinghua.edu.cn} \Leftrightarrow P$$

Optionally, the newly added DNS record can be populated to A's social network. Then A's friends or colleagues will learn A's IPv6 address and communicate with A directly. Such feature goes beyond functionalities provided by popular IM services, such as Gtalk, MSN Messenger, or QQ (yet another popular IM application in China), because TUCAN provides direct user-to-user communication at network level instead of at application layer. It helps enable the potential new people communication applications or patterns.

The TCP/IP design enables an "any-to-any" computer communication model where any two computers on the Internet can talk to each other. Such model helps the Internet growing at an unprecedented rate, however, it is also exploited by spammers and attackers. To avoid same problem in TUCAN, some research results from social network research will be explored, such as the one proposed by Davis Social Link (DSL) project [10]. DSL project integrates the social relationship into the Internet communication. Such integration provides more control to end users on who they trust to communicate, and consequently helps preventing from spam or DDoS attacks. TUCAN may adopt same idea to build inter-user communication over real-world social relationships.

IV. DISCUSSIONS

A UCI network will have different network properties which may be able to offer different services than traditional TCP/IP networks, but also may bring new issues. Due to page limit, we can only briefly discuss some of issues and potential capabilities in this section.

A. *Privacy*

By its nature, UCI faces more privacy challenge than TCP/IP networks. In some scenarios where user's privacy is only guaranteed to a certain level, UCI may be a more suitable technology. For example, it is a common practice for many companies to monitor employees' network activity for fair use of their network infrastructure. In such cases, UCI can apply usual privacy protection approaches and practices. If user's network traces are collected, such as who visited where at which time, those data should be securely guarded, and only can be accessed by authorized users. In addition, a software proxy or a shared random address pool can be used to mask out user's real identity when needed. Alternatively, users may opt to connect a regular IPv6 network if possible when privacy is a bigger concern.

B. *Backward compatibility*

Today's applications cannot take full advantages from UCI until they are modified to recognize user identities. In that sense, UCI is not backward compatible to existing applications. However, we argue that such modifications are scoped to individual applications and can be done in an incremental manner to roll out new services gradually. One way to reduce the application modification cost is to use 32bit user ID as endpoints so it can be compatible with today's TCP/IP application, as stated in Section II-A. Another possible approach is to develop some middleware modules, which sits in the middle of data path between users and the applications. The middleware understands UCI concept and can map user identities obtained from UCI networks to existing user accounts for legacy applications through a user database or something similar.

V. Related Work

Andersen et al. [4] stated that lack of network accountability largely contributed to the Internet security problems we are facing today. Accountable Internet Protocol (AIP) was proposed to replace today's IP to improve overall Internet security via self-certifying addresses. We concur on the issue of network accountability but we approach the problem from a different perspective. Moreover, our approach does not intend to change the Internet architecture, rather we focus on changes to edge networks, *i.e.*, intranets.

Chen et al. [15] proposed a User-Oriented Addressing (UOA) which related user identities to network addresses. The idea is similar to UCI, but UOA mainly addresses the namespace isolation problem in a distributed and resource-sharing computing environment, such as PlanetLab. UCI proposed a more generic network architectural change to address network security and management concerns, as well as a focus change from computer communication to people communication.

In [6], Ford et al. presented Unmanaged Internet Architecture (UIA) allowing end users to directly communicate with each other using names instead of IP addresses. Users assign locally scoped names to their mobile devices, peer with other users through social interactions, then locate and forward traffic over an overlay network. UIA focuses on providing conveniences to end users by hiding low-level network connectivity details. Compared to the ad-hoc approach explored in [6], we explored a different path to emphasize on changing the network layer to provide a fundamental basis for various applications and user cases. Guha and Francis [3] proposed a name-based signaling approach, named NUTSS, to negotiate a data path traversing middle boxes.

It has been long discussed about the idea to separate the network location information (known as locator) from the end-point identification (known as identifier) in the routing domain [11-14]. However, the definition of identifier and its role has not been well formulated. We extended the identifier idea to reach out to the end users of a network.

UCI provides a means for a single user to be uniquely identified even at application layer. This feature could potentially help resolve the same user identity management problem facing business and industry today. Proposals such as OpenID, OAuth and SAML are developed for organizations to collaborate with each other to reduce the overhead and cost resulted from user identity management. In fact, it further evidences the real-world requirement that users should be considered as part of networking architecture.

Acknowledgment

We'd like thank Lixia Zhang, Felix Wu, and Yang Yu for their valuable comments and fruitful discussions.

References

[1] Vinton G. Cerf, Robert E. Kahn, "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Vol. 22, No. 5, May 1974 pp. 637-648.

[2] D. Clark. "The Design Philosophy of the DARPA Internet Protocols". ÄCM SIGCOMM '88. 1988.

[3] Saikat Guha and Paul Francis, "An End-Middle-End Approach to Connection Establishment," ACM SIGCOMM, 2007

[4] D.G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker, "Accountable internet protocol (AIP)," Proceedings of the ACM SIGCOMM, 2008, pp. 339–350.

[5] ACK Networks Inc., http://www.acknetworks.com/

[6] Bryan Ford, Jacob Strauss, Chris Lesniewski-Laas, Sean Rhea, Frans Kaashoek, and Robert Morris, "Persistent Personal Names for Globally Connected Mobile Devices," OSDI, 2006.

[7] A10 Networks, http://www.a10networks.com/products/idseries.php

[8] RSA Press Release, "RSA Security Survey Reveals Multiple Passwords Creating Security Risks and End User Frustration", Sep. 2005.

[9] Ran Atkinson and S. Bhatti, "An Introduction to the Identifier/Locator Network Protocol (ILNP)," IEEE London Communications Symposium (LCS), 2006.

[10] L. Banks, S. Ye, Y. Huang, and S.F. Wu, "Davis social links: Integrating social networks with internet routing," Proceedings of the 2007 workshop on Large scale attack defense, 2007.

[11] Robert M. Hinden, "New Scheme for Internet Routing and Addressing (ENCAPS) for IPNG," RFC 1955, Jun. 1996.

[12] Robert Moskowitz and Pekka Nikander, "Host Identity Protocol (HIP) Architecture," IETF RFC 4423, May, 2006.

[13] Dino Farinacci, Vince Fuller, Dave Meyer, and Darrel Lewis, "Locator/ID Separation Protocol (LISP)," IETF Draft, Jan. 2010.

[14] D. Jen, M. Meisel, D. Massey, L. Wang, B. Zhang, and L. Zhang, "APT: A Practical Tunneling Architecture for Routing Scalability," UCLA Computer Science Department, Tech. Rep, 2008.

[15] Maoke Chen, Akihiro Nakao, Olivier Bonaventure and Taoyu Li, "UOA: User-Oriented Addressing for Slice Computing," In Proceedings of the 20th ITC Specialist Seminar on Network Virtualization, Hoi An, Vietnam, May 2009

[16] CERT Insider Threat Team, "CyberSecurity Watch Survey", 2011

[17] Ferraiolo, D.F. and Kuhn, D.R. (October 1992). "Role-Based Access Control", 15th National Computer Security Conference. pp. 554–563.