Wbone: WLAN Roaming Based on Deep Security

Carsten Bormann <cabo@tzi.de>; Niels Pollem <np@tzi.de>; 2003-02-25

1. The Problem

Wireless LAN (WLAN) technology is changing the life of researchers everywhere by fulfilling the dream of continuous connectivity. Today, researchers that have undergone this life change become significantly less productive when visiting other institutions -- while these may have WLANs, too, their use typically requires additional administrative action that may not be obtainable easily. Similarly, some regions may have multiple universities and other research institutions and need to allow students and faculty to flow freely between these areas of work without losing their WLAN-based connectivity.

Clearly, a technical solution is needed to allow *roaming* between places that want to allow each other's users access to their WLAN resources. Typically, the NREN customers in Europe have little qualms with hosting members of other NREN customers in their networks, as long as their security requirements are not compromised and they don't incur additional overhead. Obviously, the latter requirement can only be achieved if the roaming solution is easy to use for its end-users -- requiring an additional administrative step per roaming incidence is unacceptable. Network administrators also want to minimize the additional complexity they have to endure for enabling roaming.

Usability also means that the roaming solution must be available to existing WLAN users at low cost -- both in additional hardware and software and in system changes that may be hard for them to perform. For users of WLANs based on 802.1X authentication, such a solution is relatively easily achievable using well-understood techniques of interconnecting RADIUS backend systems [Klaas Wierenga, SURFnet, Netherlands: "Cross-organisational Roaming on Wireless LANs Based on the 802.1X Framework". TNC 2003, Zagreb.]. But what about WLANs based on L3 security ("VPN technology" or "deep security")?

In "deep security" WLANs, users don't authenticate to the WLAN, but instead are simply granted access. However, the WLAN does not connect to anything interesting (except for a few "free services", maybe) -- the only access it provides is to one or more L3 security gateways. This allows the deployment of multiple such gateways to enable access from the WLAN to departmental networks with diverging security policies. The WLAN access only becomes useful when the user can authenticate to the security gateway desired; this then allows "VPN" (virtual private network) access to the target network they desire (which may be connected to the Internet). Many academic networks in multiple European countries are using this approach as there is no such thing as a site-wide security policy that could be enforced at the L2 access level. WLAN users typically already have L3 security ("VPN") software installed to allow secure access to their desired networks from their homes or on the road; this kind of software also is available for (and often built-in with) a wider variety of client systems than 802.1X.

2. Wbone: Making Deep Security Roam

The state of Bremen currently has 5 universities/colleges and one large research institution. All but one of these use a deep security architecture on their WLANs, using an RFC1918 address range for the access network. By establishing a VPN tunnel to their institution's gateway, users obtain a routable IP address from the institution's address range.

The solution for enabling roaming within Bremen is surprisingly simple: By interconnecting their private access networks, and routing between them, the institutions in Bremen have formed the so-called "Wbone" -- actually, one large access network. Users now roam freely between the institutions' WLANs -- no new software or new security credentials are necessary; users can simply connect to their home institution's L3 security gateway as if they were there. (They do have to change 802.11b SSIDs -- a relatively small inconvenience, though.)

The actual interconnection of the WLAN networks in Bremen was quite simple, as an L2-based city network was available. One router was dedicated to the Wbone (originally, it was planned to use the "virtual routing and forwarding" capability of some routers; bugs prevented this).

Extending the Wbone to other RFC1918-based deep security WLANs now is a matter of establishing tunnels through the Internet. We are currently in the process of defining agreements for the tunneling and routing protocols needed and the address assignment and DNS policies.

3. Scaling to non-RFC1918 WLANs

Not all deep-security WLAN deployments make use of RFC1918 addresses. E.g., in SWITCHmobile, site WLANs often use routable addresses, making it much easier to interconnect them. Access control routers maintain the separation between the WLAN and the interesting networks: custom ACLs are set up to only allow access to well-known L3 security gateways. Part of the administration of the SWITCHmobile project is the maintenance of the ACLs.

Interconnecting routable WLANs and the Wbone can be done in two steps:

1. First, the L3 security gateways in Wbone sites can be provided with routable Internet addresses (which many of them already have for use from home/on the road). Once administrative methods are set up to make these addresses known to networks such as SWITCHmobile, Wbone users can roam to these networks.
2. For reciprocity, more work is required: SWITCHmobile users roaming to the Wbone cannot access their home gateways -- RFC1918 packets will not reach these. It seems unlikely that all SWITCHmobile L3 gateways will be connected to the Wbone. Instead, a more elaborate solution involving NATs is required: Packets from the roamers need to be translated to globally routable addresses and back. The NATs need to implement the same kind of ACLs in use within SWITCHmobile. Fortunately, only one such (or a small number of) NATs need to be deployed for the Wbone.

4. Conclusions and Further Work

While all the problems discussed are solvable per se, building a Europe-wide parallel Wbone Internet based on RFC1918 addresses is a controversial approach. It is generally perceived to be a massive scaling problem -- while the technologies can do it, the administration will be a significant burden. As an example, the first address assignment conflict has already surfaced between two German WLAN sites. Similarly, the ACL-based approaches scale badly with respect to the administrative effort required.

Nonetheless, the prize for pursuing this will be trans-European WLAN roaming between the sites that do implement deep security.

Obviously, further work is needed for enabling roaming between the 802.1X sites and the deep security sites. The development of 802.1X access points that allow to divert unauthenticated traffic into a separate VLAN is a promising step towards making this possible.

Acknowledgments

The authors would like to thank the members of the TERENA TF Mobility for many useful discussions on how to make Wbone and other deep security approaches work on a European scale.