Authentication, Security and Security risks

Robert G. Moskowitz

ICSAlabs

IEEE 802 Plenary Meeting

Kauai, Nov 12, 2002

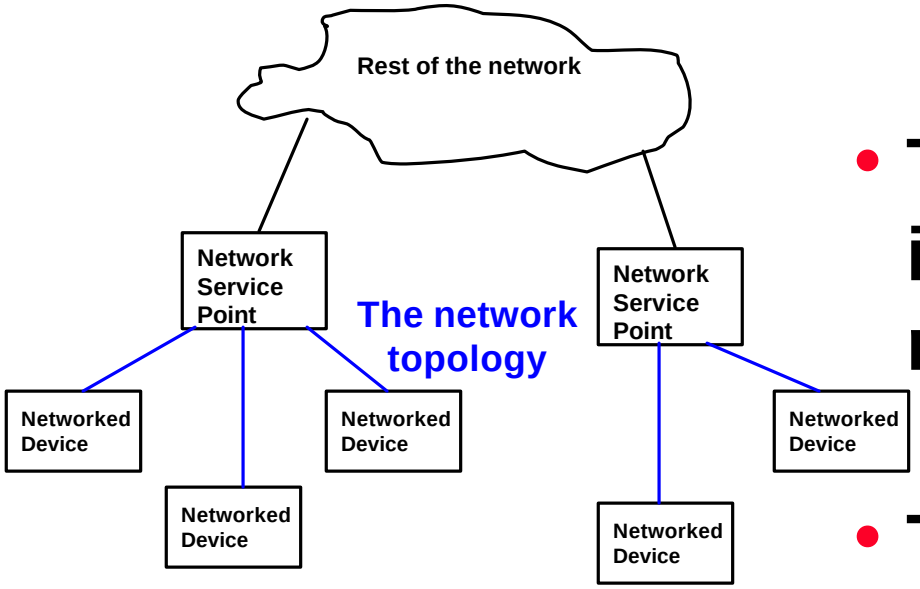
Claims

- **IEEE 802.1x is an inadequate Authentication Model for general use in 802 networks**
  - Look at 802.11 and how they are working around pre-authentication
  - Look at the billing challenges in 802.3ah
- **We really do not have an Authentication ARCHITECTURE clearly defined for 802 networks**
- **It is possible to develop an Authentication Architecture that will truly facilitate security within 802 networks**
  - What follows is an example with details and possible work

Goals

- **Define what a Network is in this context**
- **Understand Security Risks impacted by Authentication**
- **Define Authentication services in such a manner as to provide for:**
  - Media Type Independence
  - Provide for multiple provider authentication
  - Enable fast connections (i.e. fast roaming)

Network Definition



- For purposes here, a Network refers to Layer 2 and 3 services
- The network is an entity in its own right that needs to be secure
- The components of a network need various levels of security

Security Risks

- **Authentication and/or data theft**
  - Can a device intervene in the authentication and become a network user
  - Can a device intervene in the authentication and acquire all traffic from a network user
- **Disruption**
  - Disrupt the connectivity of a network user
  - Disrupt the resources of a network component
- **Resource theft**
  - Use network resources without payment
  - Consume limited network resources to the detriment of authentic network users

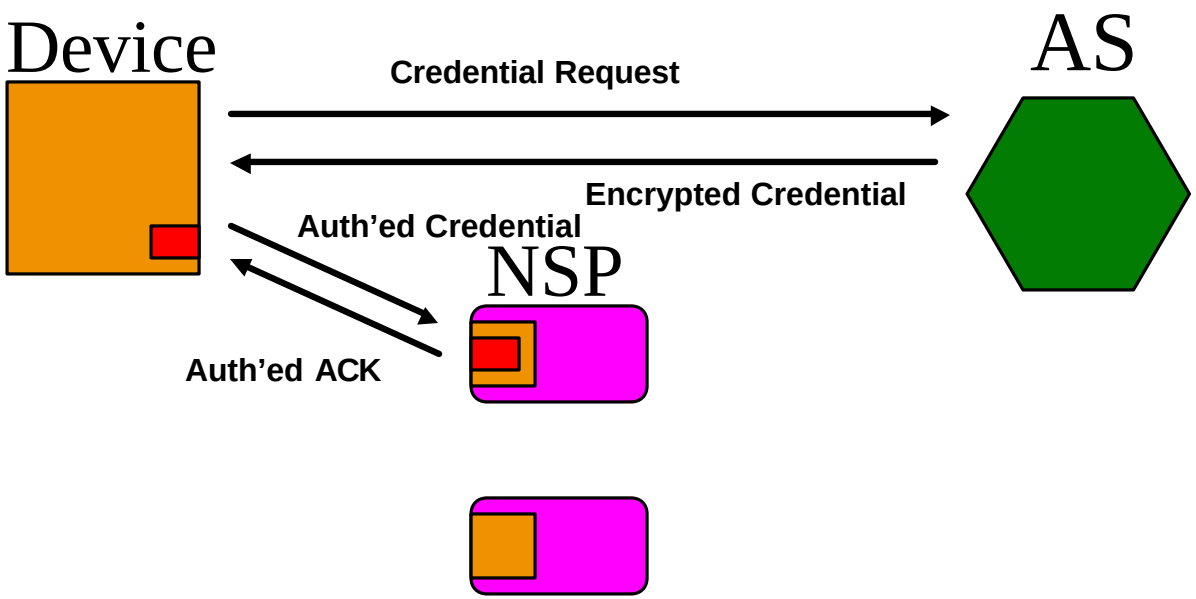
The Need for Authentication

- **Authentication MUST occur at multiple levels within a Network**
  - Even when only layer 2 is considered
  - If Authentication is layered, then Network services can be more appropriately controlled, billed, and managed.
- **Authentication services MUST identify all involved parties**
  - This includes Multicast situations
- **Authentication is the bootstrap for other security services**

Security with Authentication

- **If Authentication does not directly involve all components, every step built off the Authentication is at risk**
  - This can be met with an Needham-Schroeder based methodology
- **Authentication should directly enable other security services**
  - i.e. provide keying material to involved parties

Needham-Schroeder



Advantages Gained

- **Potential Billing points**
  - At Device authentication to AS
  - At Device request for credential(s)
  - At Device presentation of credential(s) to NSP
- **NSPs are assumed to be within a network**
- **Device COULD authenticate to another network thru current network if there is a business relationship**

Summary

- **By changing the Authentication architecture MOST of the requirements coming out of the various 802 groups can be facilitated**
- **The Authentication architecture proposed here COULD be provided by**
  - An enhancement to 802.1x
  - An enhancement to EAP
- **Needham-Schroeder is well understood within the security community and MOST EAP methods could be extended to provide this sort of authentication**