

Towards a Federated Security Model for Authentication/Authorization in Videoconferencing over Internet2



Samir Chatterjee

School of Information Science
Claremont Graduate University

&

Member: VidMid-VC working group

<http://middleware.internet2.edu/video>



Outline of Talk

- VidMid Activities
- Presenting the components of VC
- A proposed Security Framework
- Threat Models
- Synergies with AG
- Future



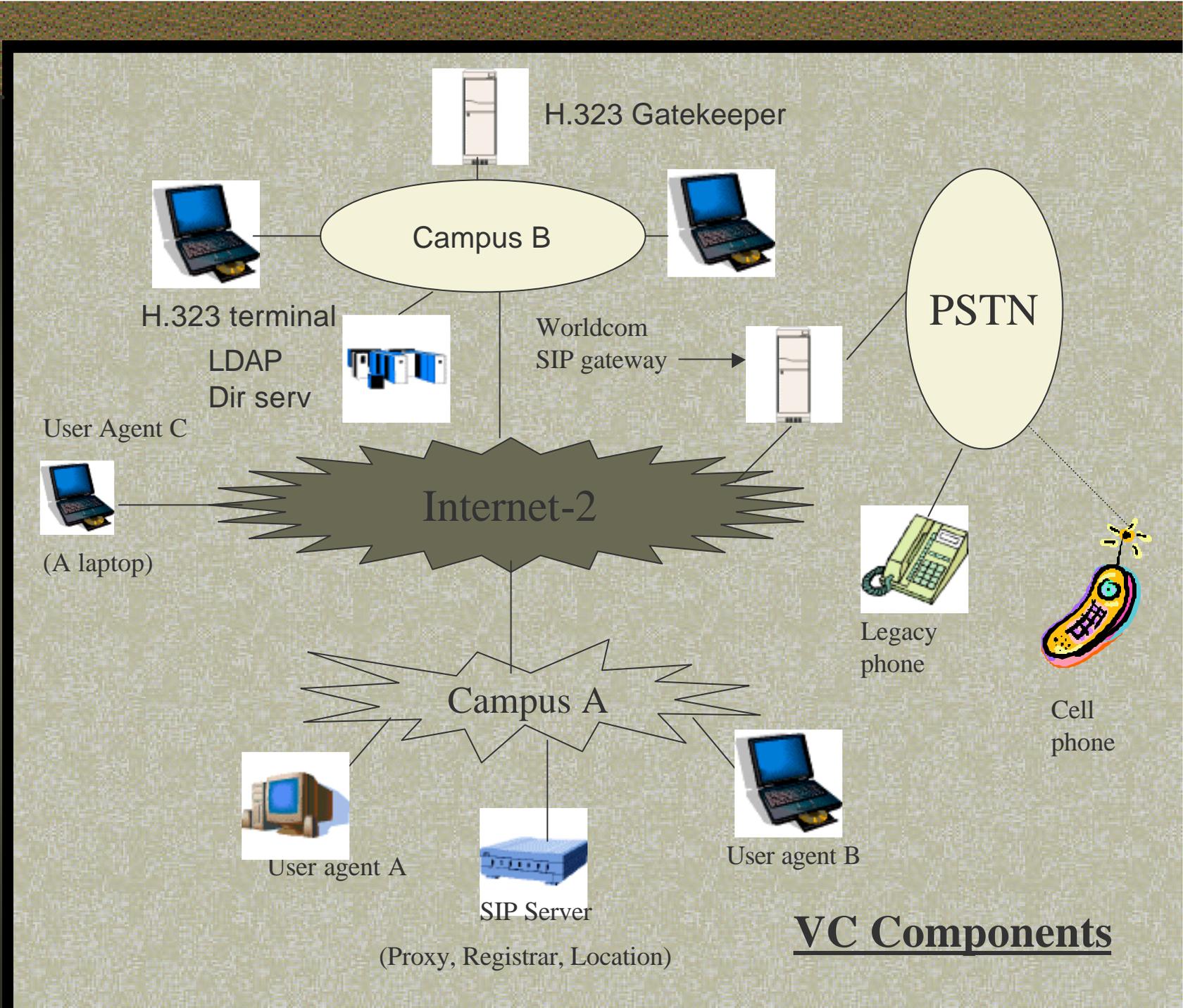
Internet2 VidMid activities

- August 2001 – Creation of VidMid-VC and VidMid-VOD
- November 2001 – UNC, Chapel Hill Meeting of VidMid-VC members
- Scenarios for Videoconferencing
 - <http://middleware.internet2.edu/video/draft-internet2-vidmid-vc-prioritized-workplan-scenarios-00.html>
- January 2002 – Security Framework
 - <http://middleware.internet2.edu/video/draft-chatterjee-johnson-vc-security-01.html>
- January 2002 – ComObject specs for VC resources
 - <http://middleware.internet2.edu/video/draft-johnson-h323-ldap-infra-01.doc>



Why middleware for VC?

- Middleware-enabled VC will enable a researcher to look up a colleague or a conference by name and find a “click to connect” link.
- That link will result in authenticated and perhaps encrypted by-directional, multimedia session at the remote person’s current location and on their conferencing equipment of choice using their protocol of choice.
- We do not want any central authentication server. Instead we seek a federated model where cross institutional authentication/authorization can happen via directory servers.
- There are no commercial VC products today that can do that.

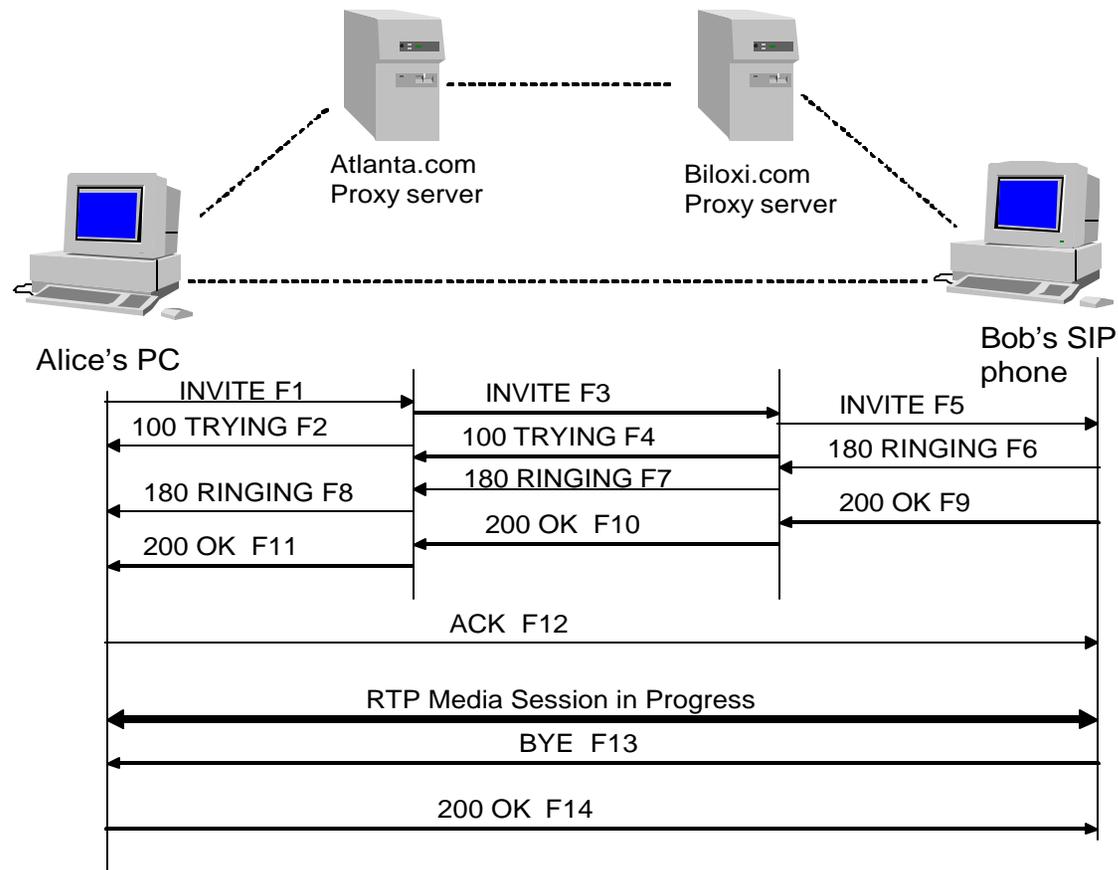




Security Framework

| | |
|-----------------|---|
| Authentication | is means of identifying another entity. There are many ways to authenticate another entity, but the typical computer based methods involve user ID/password or digitally signing a set of bytes using a keyed hash |
| Confidentiality | Cryptographic confidentiality means that only the intended recipients will be able to determine the contents of the confidential area |
| Integrity | A message integrity check is means of insuring that a message in transit was not altered |
| Authorization | Once identification of a correspondent is achieved, a decision must be made as to whether that identity should be granted access for the requested services. This is the act of authorization. This is often done using access control lists (ACL). |
| Privacy | They want to make sure others do not know what they are doing or transmitting. Some people prefer anonymity. In a higher education environment, faculty and student reserve the right to privacy. |
| Non-repudiation | Reverse protection |
| Administration | Billing and accounting, maintenance of Call Data Records (CDRS) |
| Audit-trail | Do not shred documents – Enron! |

SIP – the IETF Standard





Classic Threat Models

- **Registration Hijacking** – A registrar assesses the identity of a UA. The From header of a SIP request can be arbitrarily modified and hence open to malicious registration.
- **Impersonating a server** – A UA contacts a Proxy server to deliver requests. The server could be impersonated by an attacker. Mobility in SIP further complicates this.
- **Tampering** with message bodies



More threats

- **Tearing down sessions** – insert a BYE
- **Denial of Service attacks** - Denial of service attacks focus on rendering a particular network element unavailable, usually by directing an excessive amount of network traffic at its interfaces. In much architecture SIP proxy servers face the public Internet in order to accept requests from worldwide IP endpoints. SIP creates a number of potential opportunities for distributed denial of service attacks that must be recognized and addressed by the implementers and operators of SIP systems



Authentication Implementation

- SIP provides a stateless challenge-response mechanism based on HTTP style
- There are two types:
 - basic authentication (ID and password in the clear)
 - digest authentication (uses cryptographic hashes)
 - UA to UA, UA to Proxy

WWW-Authenticate: Digest

```
realm="biloxi.com",  
qop="auth,auth-int",  
nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",  
opaque="5ccc069c403ebaf9f0171e9517f40e41"
```



Other Security Issues

- Full encryption of SIP messages (using IPSEC, TLS, S/MIME)
- SIP requests and responses cannot be simply encrypted end-to-end since there are many header fields that must be visible to proxies for routing SIP messages. Note that proxy servers need to modify some features of messages (such as adding Via headers) in order for SIP to function.
- Apply encryption at various layers: S/MIME, TLS and IPSEC



Authorization Challenges

- ACLs — the read/write/execute controls that are embedded in file systems
- New approaches - Traditional access control models are broadly categorized as discretionary access control (DAC) and mandatory access control (MAC) models. New models such as role-based access control (RBAC) and task-based access control (TBAC) have been proposed to address the security requirements.
- VidMid exploring other solutions



Shibboleth (MACE/IBM)

- Shibboleth's solution is to have users registered only at their origin site, and not at each resource provider site
- A critical component that is needed for privacy is the Attribute Authority (AA).
- AA also has the responsibility of providing a means for users to specify exactly which of their allowable attributes gets sent to each site they visit
- For SIP and H.323 systems, we envision directory name lookups and resource discovery done by Shibboleth way



Future

- Access Grid Synergies
- User versus device authentication?
- Traversing NAT and Firewalls
- Integrating with policy managers
- Implementing QOS and video codec optimization
- Any other ideas??

Thank You!