MINUTES -- IRTF SMUG MEETING -- March 1999 (IETF44)

DAY ONE - Monday, March 15, 1999, 3:30pm - 5:30pm

Introduction

Ran Canetti

Presentations

Slides at http://www.ipmulticast.com/community/smug

D. Balenson (TIS): Key Management for Large Dynamic Groups

G. Tsudik (USC): An overview of CLIQUES key agreement protocols

Y. Shavitt (Bell-labs): A key management scheme for multicast

I. Monga (Nortel): Proposal for Group Security Association

M. Kadansky (SUN): Security issues in designing Reliable Multicast protocols

DAY TWO - Tuesday, March 16, 1999, 9:00am - 11:30am

Moderator: Thomas Hardjono

Agenda

- Review Charter, goals (short term, long term), IRTFs
- Building blocks approach
- Data-stream encryption: IPsec based (L3) or L4/L7
- Key management:
  - at L4 or L7
  - Single server multiple/distributed servers
- SMuG Plans / Roadmap / Timetable

REVIEW CHARTER

SMuG main goals are to:

1. Define a coherent taxonomy for multicast security
2. Identify prominent scenarios, the problems involved, and their overlap
3. Define security requirements for the prominent scenarios

4. Design initial prototypes for secure multicast in one or more of the prominent scenarios.

There are many different ways of looking at multicast security, and many different security requirements depending on the application. The wide range of views has made it difficult for the IETF community to come to consensus on how to proceed. The proposed research group will have two main goals First, to identify the security requirements of prominent multicast applications, and the properties required from solutions. Second, to design (one or more) prototypes of secure multicast systems for a chosen prominent application (or set of applications). The stress will be on simplicity and workability. Once ready, the prototype(s) will be forwarded to the IPSEC (or another) working group of the IETF for standardization.

DISCUSSION:

Are prototypes within scope of an IRTF RG? IRTF guidelines focus on research and are vague on topic, but should be ok. Some precedent, e.g., PSRG developed PEM before handing over to PEM WG.

Discussion of Reliable Multicast research group?

Balenson comments on charter.

This charter has been approved by IAB.

Can change and evolve over time.

A FIRST-CUT SOLUTION: PAST DECISIONS

One-to-many communication. [Many-to-many later.]

Trust a single (centralized?) group manager, having one or more key-servers.

Need source authentication.

Need to handle dynamic group membership.

Secure multicast group is independent of IP multicast group. That means: joining the SMuG is done independently of joining IP multicast group; routing of data packets is independently from SMuG; (data) crypto is done only at endpoint.

DISCUSSION:

Thomas: received some calls/emails regarding whether IRTF should develop first-cut solution so quickly. Don’t want to solve part of the problem too quickly at the expense of others.

Canetti: do both things in parallel, short-term solution, and continue long-term research.

Dinsmore: we've skipped a step - what's the framework/architecture.

???: There is one draft w/ some architecture.

Canetti: First join IP multicast group for routing, then join secure group by registering with manager; then get keys. SO, IP multicast group always superset of secure multicast group.

Thomas: For data don't need translation, but might need it for key management.

Bellovin: broadcast model, like premium cable channels, long history of people reverse engineering; here crypto in endpoint in software, so makes possible for one bad endpoint to get and distribute key to others. Bandwidth is a resource as well, and may need crypto to join it. Separate multicast security issue. What about using different keys or shifting keys at different points to thwart getting the key?

Thomas: problem is really with basic multicast model. IGMP doesn't send any info. Just gets there. Anyone can join, without the sender realizing it. Like satellite in some ways.

Bellovin: though different here since shared resource so limited bandwidth.

Thomas: like Real Player viewer? DVD players coded for different regions.

Thomas: so, should endpoint encryption point be a question mark?

???: reason for consensus in past because scalable?

Thomas: RM people looking at authentication of control packet and how that should work. Leaving content security to us. So, a first-cut solution for data-stream encryption would be needed.

REFERENCE FRAMEWORK SLIDE & BUILDING BLOCKS

Simplicity inspired by Policy WG.

Ignoring problems first, the Framework identifies two segments corresponding to centralized designs and distributed design. Sender dealing w/ receiver in 1-to-M or M-to-M multicast. Senders/receivers get keys from key server. Another situation w/ multiple key servers, for receivers located remotely, so can't use single point.

Identify 3 problem areas:

Problem Area 1 (red): multicast data handling,
encryption/decryption, packet formats IPsec?, etc.

Problem Area 2 (blue): group-key management, SA management,
parameters management, etc.

Problem Area 3 (green): policies, policy creation, dissemination,
enforcement, maintenance, etc.

(Thomas will provide on email list as PDF file).

DISCUSSION:

Key server? Key manager? Group manager?

Policy server? Management? Administration?

Data, control, and management planes.

REASONING FOR BUILDING BLOCKS APPROACH

Standardize building blocks for Secure Multicast Protocols.

Standardize Secure Multicast Protocols built from these
building blocks.

This approach allows new Secure Multicast Protocols to be
standardized later with minimal effort.

This approach also allows new (better) building blocks to be
standardized later to replace existing ones.

Promotes interoperability

Lessons learned from RM IRTF:
Extracting "building blocks" from a near-mature protocol is painful.
Need a Reference Framework encompassing the building blocks.
Don’t leave it until its too late.

DISCUSSION:

Mark: so want APIs, too, right? Yes, must define boundaries and
interfaces.

IDENTIFYING BUILDING BLOCKS (OPENING LIST) (WRT REFERENCE FRAMEWORK)

Area-1: Data-stream security (Red area)
Building blocks for IPsec solution
Building blocks for L4/L7 solution
Others???

Area-2: Key management (Blue Area)
   Key generation block(s)
   Building blocks for key hierarchy (e.g., LKH, OFT, etc.)
   Building blocks for key dissemination:
      centralized (1 server) - define scope
      distributed - define scope
   Others???

Area-3: Policy (Green Area)
   Building blocks for:
      group key management
      access control
      compromise recovery
      SAs and GSAs
      "meta"-policies
      Others???

DISCUSSION:

Canetti: Source authentication? What layer? IPsec? Or Layer 7??

Bellovin: some implementation issues wrt IPsec key management "trusted" process on generic multi user system. Might have implications for message flows?

Tsudik: two different planes of authentication

Thomas/Bellovin: a lot of ways to potentially do source authentication. People need to explore.

GOALS AND TIMETABLE

   Problem statement and scope document (July '99)
      Written wrt Reference Framework

   Applications taxonomy document (?)

   Identification of building blocks: (July '99 (?) Now?)
      Clear purpose, functionality & assumptions
      Clear boundary(ies)
      Clear input/output & behavior-upon-input
      Relationship & dependence on other building blocks
      Message exchanges & message composition, etc.

   Separate documents / IRTF Drafts: (From July '99 to March 2000 ?)
      (ie. Write a separate document for each building block)
      Where it fits in the Reference Framework
      State assumptions & dependencies wrt other
         parts ("Problem Areas") of the Reference Framework
      State things NOT covered by building-block

   Identify building blocks which have immediate use (Dec '99 ?)

Eg. those for Reliable Multicast IRTF

"Volunteers" - commitments

DISCUSSION:

Canetti: need to discuss were we want to go for the first cut solution. Should we look at IPsec solution? Or Layer 7?

Thomas: People “paste” their interpretation on the Reference Framework to identify their building blocks. Different groups/vendors may come up with their own building-block. It is OK for two (or more) building blocks to be proposed to do the same thing (eg. encryption at L3 and L7).

Start discussing blocks on the mailing list.

NEXT MEETING?

Sunday meeting before next IETF in Oslo? Must confirm with IETF staff.

Separate question of interim meeting before next IETF. Discuss on mailing list.

PARTICIPANTS (unordered list)
============
David Balenson, TIS Labs at Network Associates
Mark Baugher, Intel
Steve Bellovin, AT&T Research
Uri Blumenthal, IBM Research
Brad Cain, Nortel
Ran Canetti, IBM Research (Co-Chair)
Pau-Chen Chang, IBM Research
Peter Dinsmore, TIS Labs at Network Associates
William Dixon, Microsoft
Thomas Hardjono, Nortel (Co-Chair)
Ross Finlayson, Live.Com
Mirian Kadasky, Sun Microsystems
Amit Kleinmann, NDS
Michael Luby, Digital Fountain
Cheryl Madson, Cisco
Inder Monga, Nortel
Tim Moore, Microsoft
Carl Muckenhirn, SPARTA
Dimitrios Pendarakis, IBM Research
Bob Quinn, Stardust
Yuval Sharitt, Bell Labs
Rodney Thayer, Internet Devices
Gene Tsudik, USC/ISI
Brian Weis, Cisco

Howard Weiss, SPARTA
Brian Whetten, Talarian
Brian Witten, Air Force Research Lab
