link layer security

Network Mgmt/Sec.

Jim Binkley

Outline - mostly ppp

- intro
- ppp/chap/ppp encryption
- radius
- 802.1x
- summary

physical link-layer security

- hw/sw known to exist
- may be arbitrarily fast in hw
  - and include encryption/session-key services
- “bump in the wire”
- pros: typically pt. to pt. “outside” link can be taken care of sans stack software complications

cons:

- may not make sense in broadcast (ethernet-like) setting
  - due to same key everywhere - more sites with secret, less of a secret
  - hard to update keys, pt. to multipoint
- by definition is not end to end, just one link
  - NOT Internet end to end security ...

broadcast domain

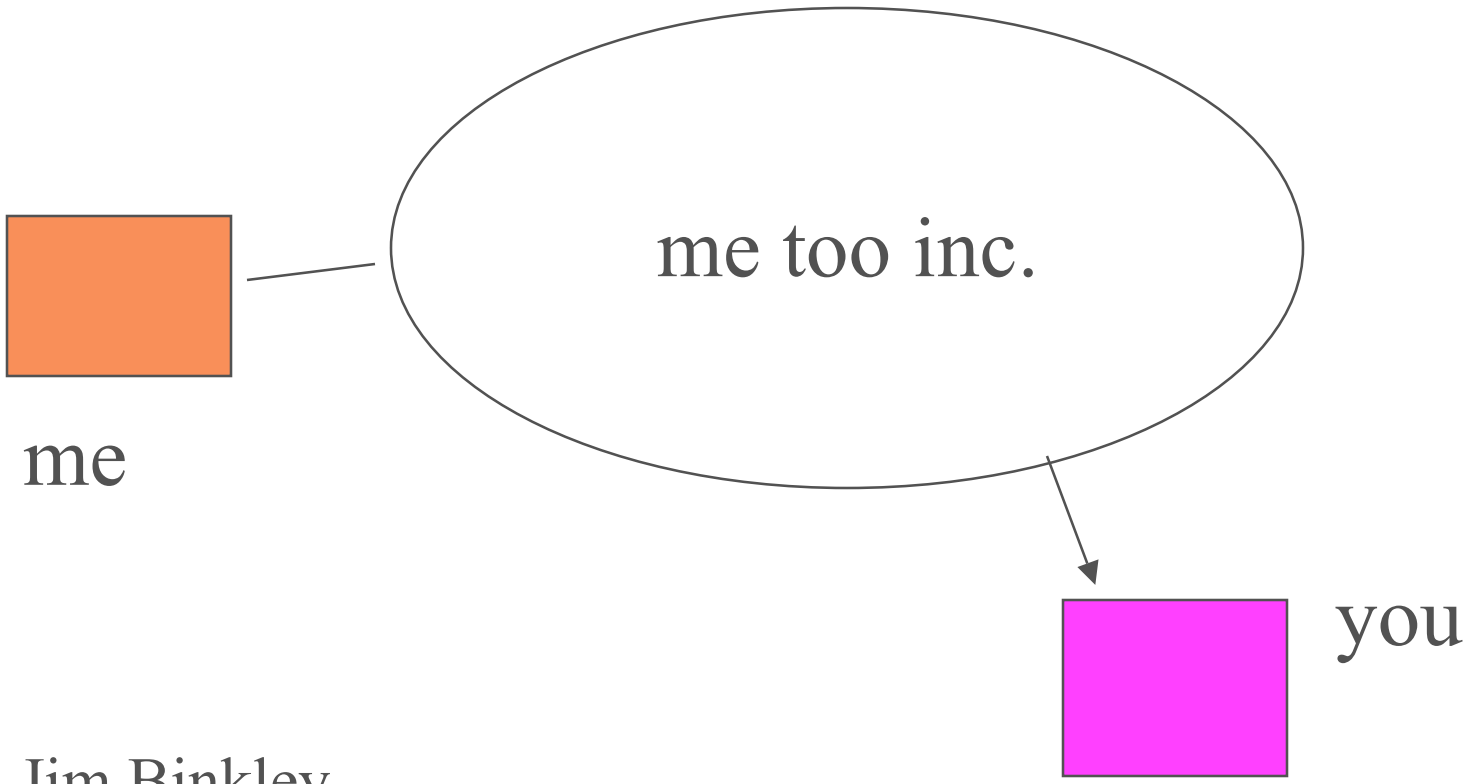
- key distribution is a problem
- leads to:
- same key everywhere
  - if everybody has the same key ... not a secret
- can be just as hard to make sure everybody has their own key
  - or own certificate
  - certificate distribution is always non-trivial

L2 trust policy not always clear

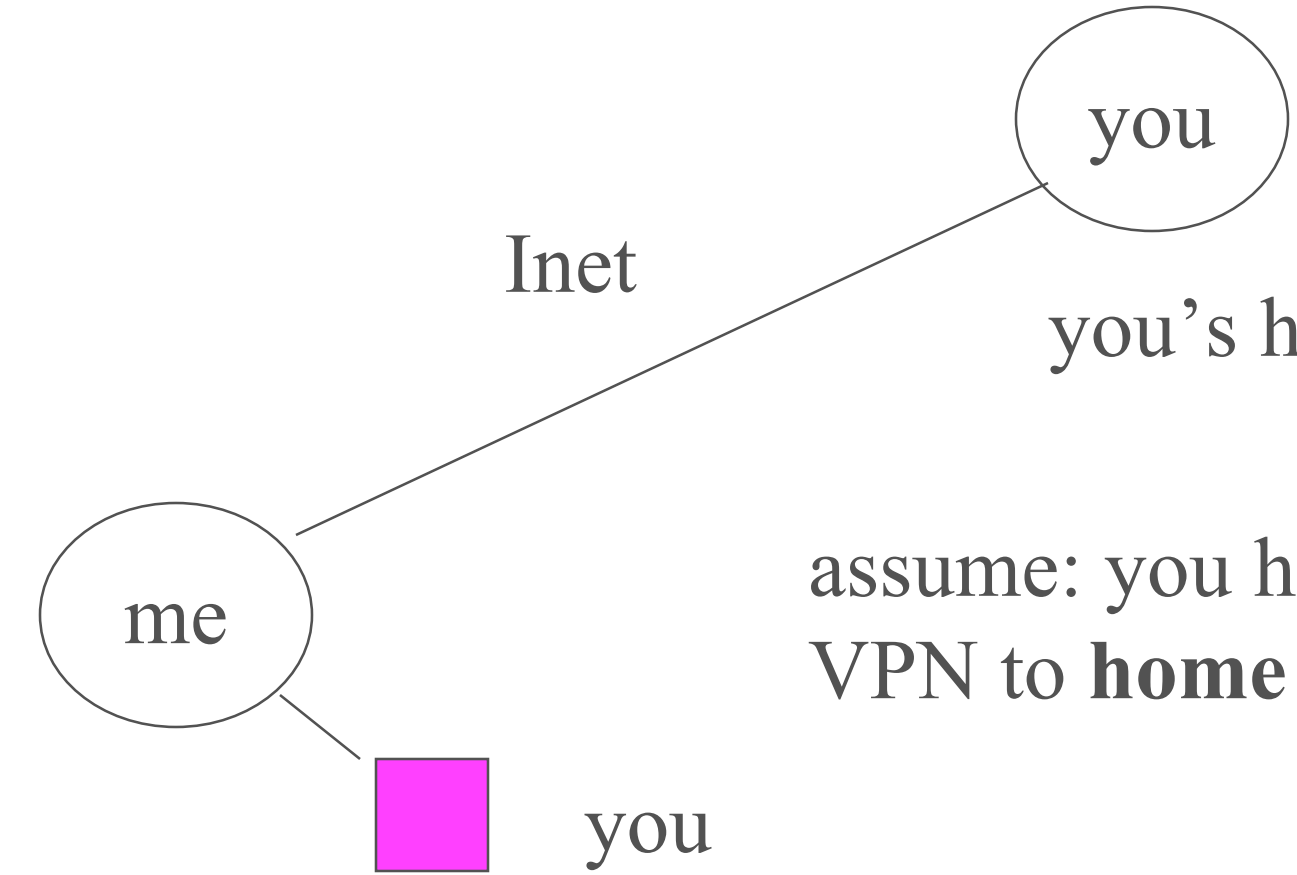
- consider PSU ... 23000 students
- what would it mean for every student to have a PSU key
- IT management nightmare
- still must have inner zone of trust?
- what if PSU wants to enable non-PSU people to use the network?
  - party A at party B domain ... maybe L2 not the ticket?

L2 secure domain

not clear: what does L2 security do for **you ?**



compared to this



PPP/security

- RFC 1661, “The Point-to-Point Protocol (PPP), William Simpson (editor), 1994
- RFC 1321, “The MD5 Message-Digest Algorithm, Rivest/Diusse, 1992
- RFC 1994 “PPP Challenge Handshake Authentication Protocol (CHAP)”, Simpson, 1996
- RFC 1968, “The PPP Encryption Control Protocol (ECP)”, Meyer, 1996
- RFC 2284, “PPP Extensible Authentication Protocol (EAP), Blunk, Vollbrecht, 1998.

PPP/security

- RFC 2419, “The PPP DES Encryption Protocol, Version 2, (DESE-bis), Sklower/Meyer, 1998
- RFC 2420, “The PPP Triple-DES Encryption Protocol (3DESE), Kummert, 1998

PPP protocol

- has two stages Link Control Protocol (LCP) and Network Control Protocol (NCP)
- provides encapsulation for data + control packets for setup
- LCP - negotiates open/close link establishment followed by
  - optional authentication stage (PAP/CHAP)
- NCP - handles network specific parts, e.g., IP address determination for NCP/IP

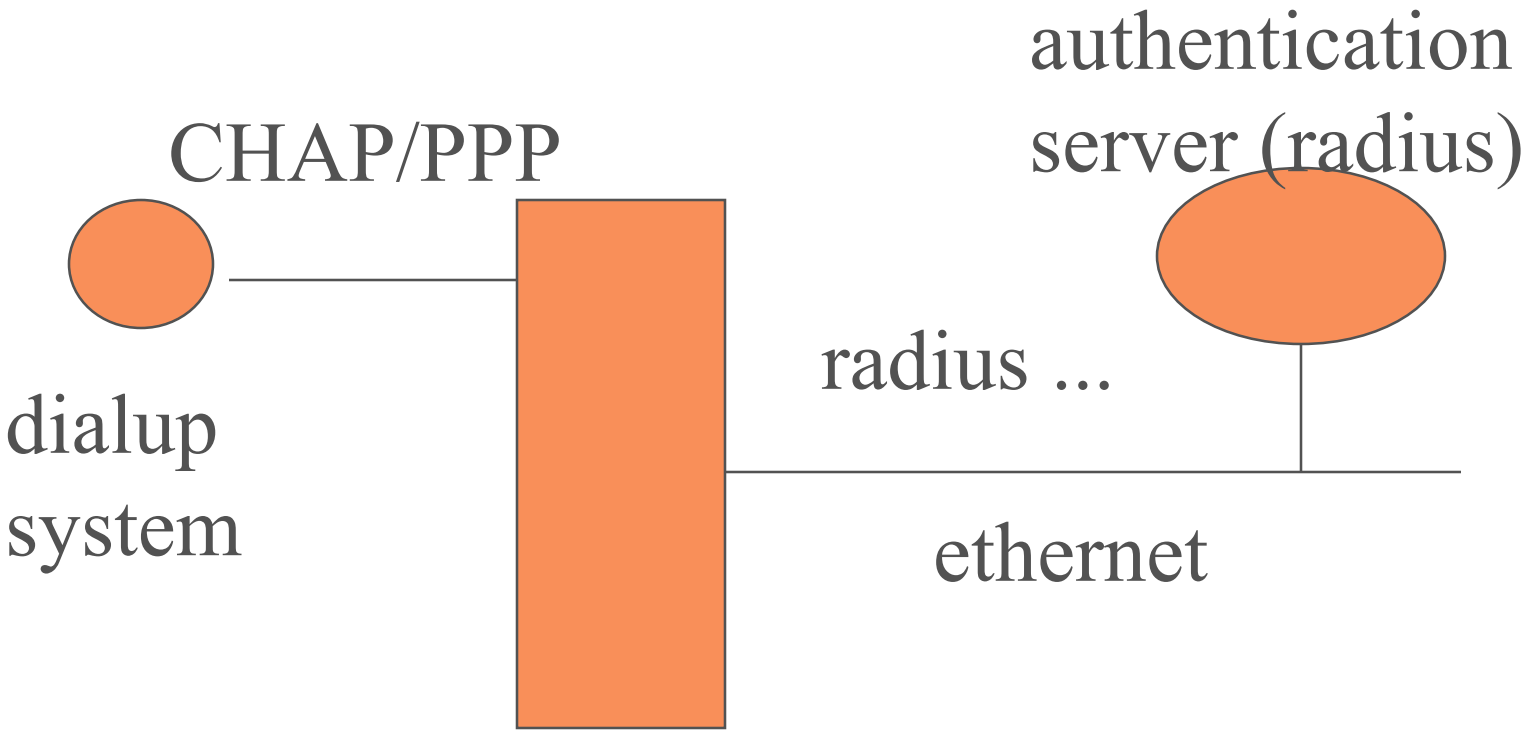
so PPP may include

- PAP - plaintext password mechanism
- what's wrong with that?
- "nobody can tap you over the phone line right?"
  - merging of voice/data takes us where?
  - security of phone infrastructure is known to you?
- just one more password in the clear
- what about data confidentiality?

CHAP overview

- essentially a challenge-response protocol between terminal multiplexor and dialup system over pt. to pt. physical link
- client must authenticate itself to enclave system
- based on shared secret and MD5 one-way hash function + “random” challenge
- CHAP is LCP authentication sub-protocol

authentication system setup



CHAP messages/protocol

- CHALLENGE, RESPONSE, SUCCESS, FAILURE
- CHALLENGE(challenge id, random #), term mux to dialup node
- RESPONSE(challenge id, response value, name)
  - hash(id, random #, shared secret) is response value
- SUCCESS or FAILURE sent back
  - term mux must run same hash with same shared secret to prove that peer has shared secret
- name likely login name, but other naming
  - other schemes are possible (just a string)

HI (old) CHAP, cont.

- name is a backend database key
  - (name, shared secret, other possible attributes)
- radius is a protocol for fetching dialup attributes in a remote server database to possibly multiple term mux/routers
- with md5 key could be 128 bit bit-string (same size as hash), although could be password derived md5hash(password)

important note:

- re CHAP
- one client, one shared secret with server
- not per network shared secret
- more secret better, because if one lost, not all are cracked

PPP Encryption Control Protocol

- RFC 1968 - basically exists to
  - 1. configure as LCP option which encryption protocol will be used (DES or 3-DES)
  - 2. and then encapsulate the data itself
- uses LCP option negotiation mechanism
- occurs when NCP protocol phase is reached
- must converge on mutually accepted encryption algorithm
- must happen before data is sent .... (obviously)

words worth heeding

- from Security Considerations part:
- “The strength of the protection is dependent on the encryption algorithm used and the care with which any ‘secret’ used by the encryption algorithm is protected.”
- “It must be recognized that complete security can only be obtained through end-to-end security between hosts.”

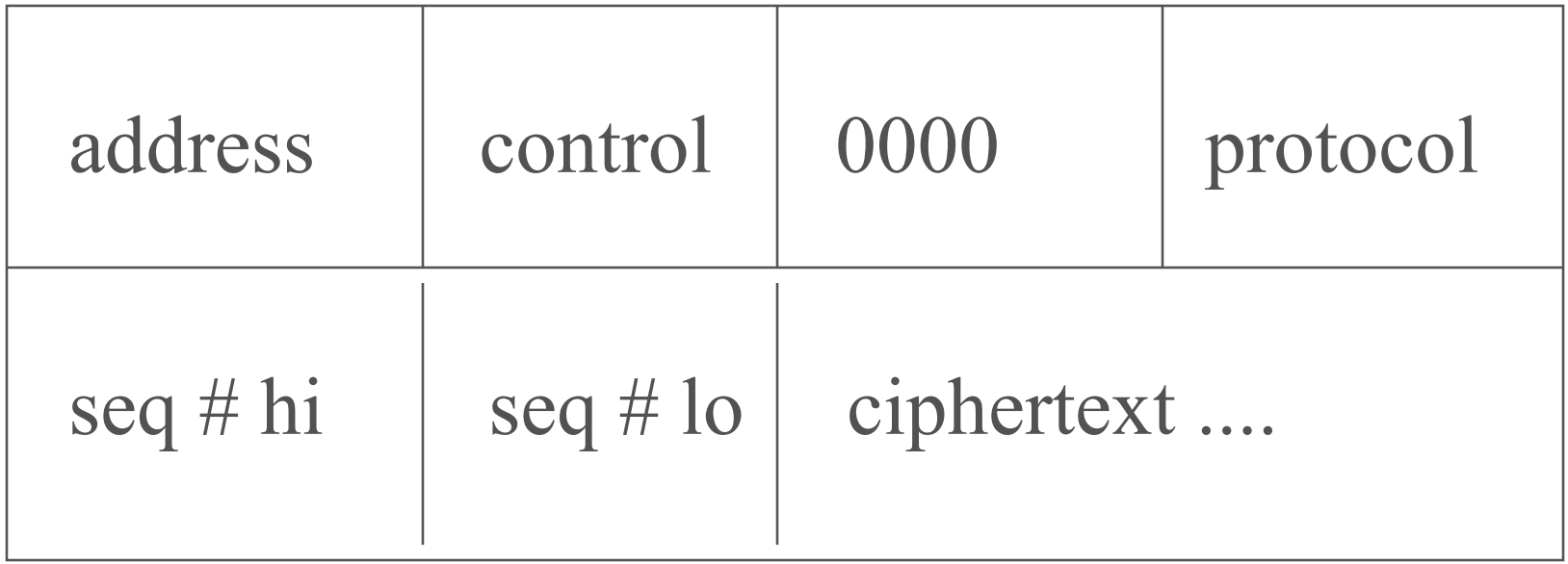
3-DES packet formats

option time configuration packet:

type	length	nonce

type: 2 meaning 3DES
length: 10 (bytes)
nonce: 8 bytes IV applied to 1st pass of algorithm

bulk data (in ppp encapsulation)



protocol id: e.g., 0x53 means individual link encryption

notes:

- 1. compress before encryption as encryption tends to defeat compression
- 2. no authentication (other than at startup say with CHAP)

radius

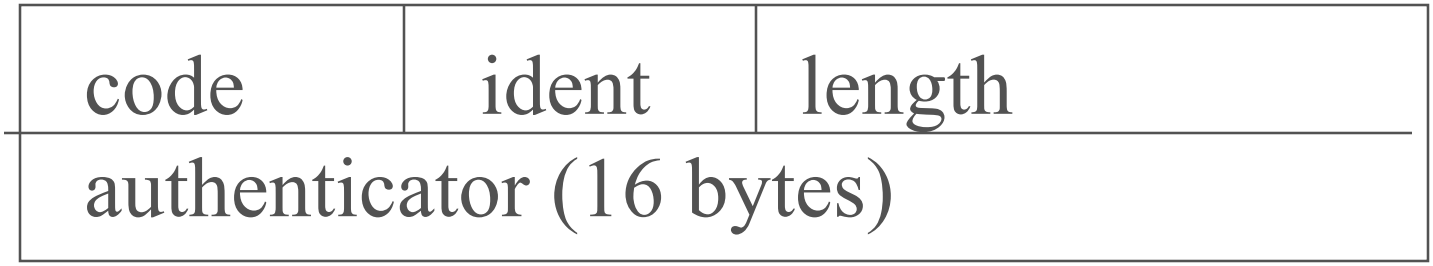
- **Remote Authentication Dial In User Service**
- RFC 2865, RADIUS basics
- RFC 2866, accounting, and on
- thru 2869
- note AAA, new protocol, RFCs 2903-6

radius

- client/server model protocol
- ties authentication/login/misc. attributes server-based database to NAS
- multiple possible “Network Access Servers” (NAS) systems (term muxen ...)
- which in turn may glue to higher-level directory system (LDAP/NIS, whatever)
- can su pport unix login/pap/chap, and suggest ppp/slip, whatever, do accounting, provide billing info

radius, cont.

- uses UDP ports
- packets all have T/L/V format for attributes
- radius servers may be duplicated and/or have other radius servers to redirect to
- packet format overall:



attributes follow ...

radius, cont

- protocol itself protected with client/server shared secret
- passwords hidden so they cannot be intercepted
- attributes stored in database can include:
  - user/passwords/framing protocol/callback-number/address info/vendor specific attributes,
  - etc.

802.1x

- IEEE proposal based on IETF RFC/s
- may be applied to broadcast/PPP dialup, 802.11
- 802.11 WEP is a failure
  - rc4 plus protocol, encryption only
  - flawed ... for a number of reasons
  - plus one encryption algorithm in firmware is a flaw in and of itself
  - plus one shared key for all users

802.1x bibliography

- rfc2284 - PPP Extensible Authentication Protocol (EAP)
- rfc 2716 - PPP EAP TLS authentication
- IEEE 802 web page:
  - http://grouper.ieee.org/groups/802/dots.html

overview

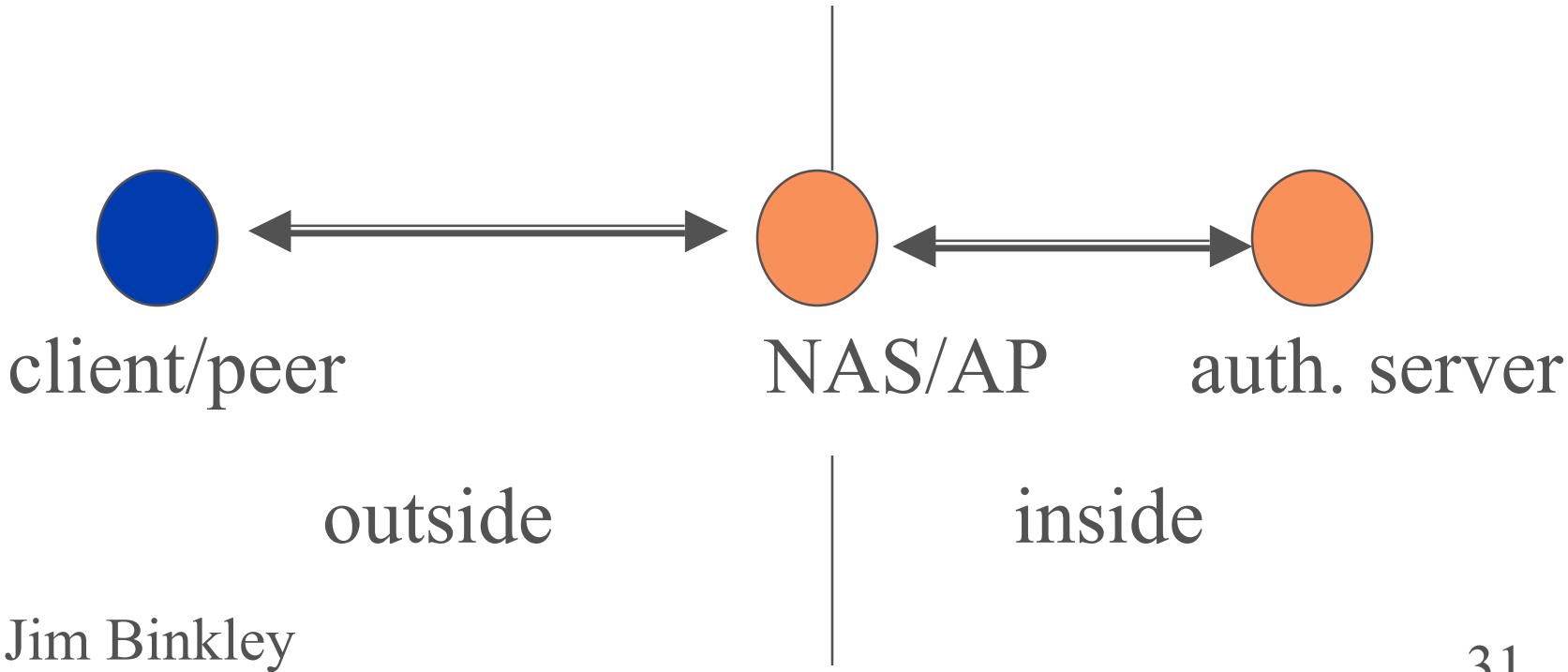
- can be used on any link, broadcast, dialup
  - ethernet/802.11
- does not have to be PPP based
- if PPP, then
  - link layer phase (LCP)
  - authentication phase (mostly her)
  - network parameter phase(NCP)

goals

- for dialup, authentication of client to server
- possible authentication mechanisms:
  - 1. md5-challenge (like chap)
  - 2. one time password (see RFC 1938)
  - 3. hw token based
- TLS mechanism adds
  - 1. session keys for encryption
  - 2. 2-way authentication

rough protocol idea

- client/backend server, NAS or AP forwards
  - and will deny service if authentication fails



link-layer pros/cons

- pros - can be done in HW easily
  - may be faster than other mechanisms
- cons -
  - historically has been flawed
    - » poor protocols + design
    - » poor key management - hard to centralize
  - not end to end
    - » subject to proposed/known plaintext attacks

802.1x framework

1. client sends EAP-start message

2. ap/server sends EAP-request id message

3. client sends EAP-response packet with id to auth. server

4. auth. server uses 1 of N auth. algorithms depending on EAP auth type (more pkts here)

    some auth. protocol

5. auth server sends EAP-success at end

EAP + TLS?

- EAP is a meta-authentication algorithm
- designed for PPP but can be used elsewhere
- internally we still need: kerberos, or chap, or hw token, or one-time password or digital signature or you-tell-me
- also at end can tie in TLS-based session-keys for encryption of packets