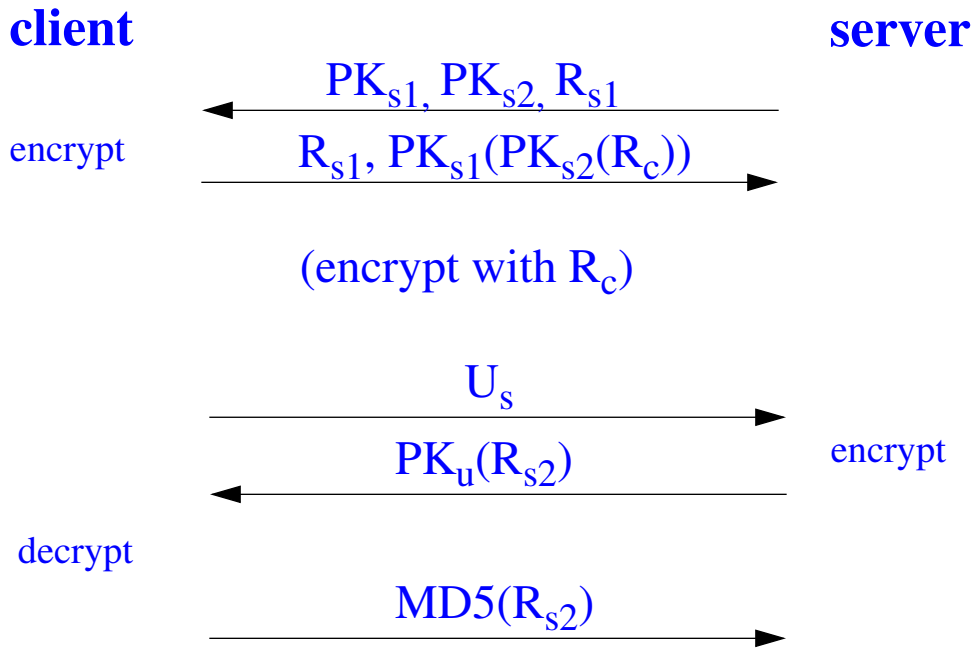
Status

- Coding versions of Telnet and FTP
- Future work: code “secure inetd server”

SSH Design


client
server
PK_{s1}, PK_{s2}, R_{s1}
encrypt
$R_{s1}, PK_{s1}(PK_{s2}(R_c))$
(encrypt with R_c)
U_s
$PK_u(R_{s2})$
encrypt
decrypt
$MD5(R_{s2})$

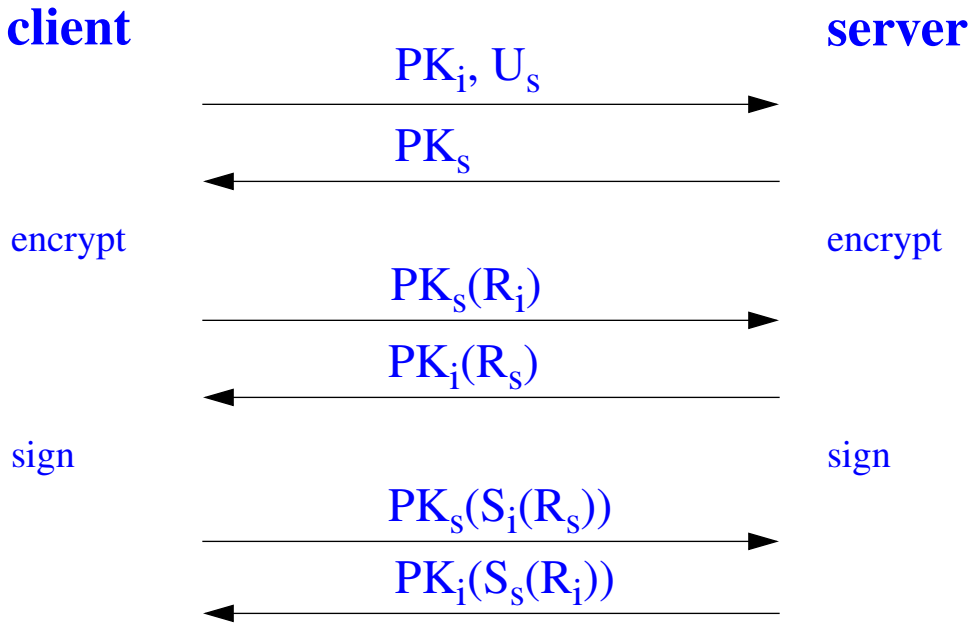
Comparison to other systems

- Diffie-Hellman based:
  - SRA
  - STEL
  - ESM
- RSA based:
  - SSL - requires CA registered certificates
  - DASS - kerberos model tickets/server
  - SSH - most interesting
    - raw RSA keys tied to account
    - no true challenge of server
    - session key determined only by client
    - rsh specific, not interoperable with existing tools

Key Management Policies

- Client and Server are free to:
  - Insist on valid keys on existing keyring
  - accept keys from secure DNS
  - accept transmitted user key based on password (once)
  - accept transmitted keys without validation

NATAS Basic Design



(encrypt with R_i ^ R_s)

NATAS Goals

- Use RSAREF
- Use authenticated PGP keys
- Separate concepts of individual from account
- Unify encryption, authentication, and authorization
    - avoid extra authentication calculations
    - single point of authorization
- Compatibility with telnet, FTP, ESP
- Multi-hop support
- Secret key never leaves individual desktop

SRA Limitations

- No server authentication
- unauthenticated keys allows active man in middle attack
- short key length of Sun's Secure RPC

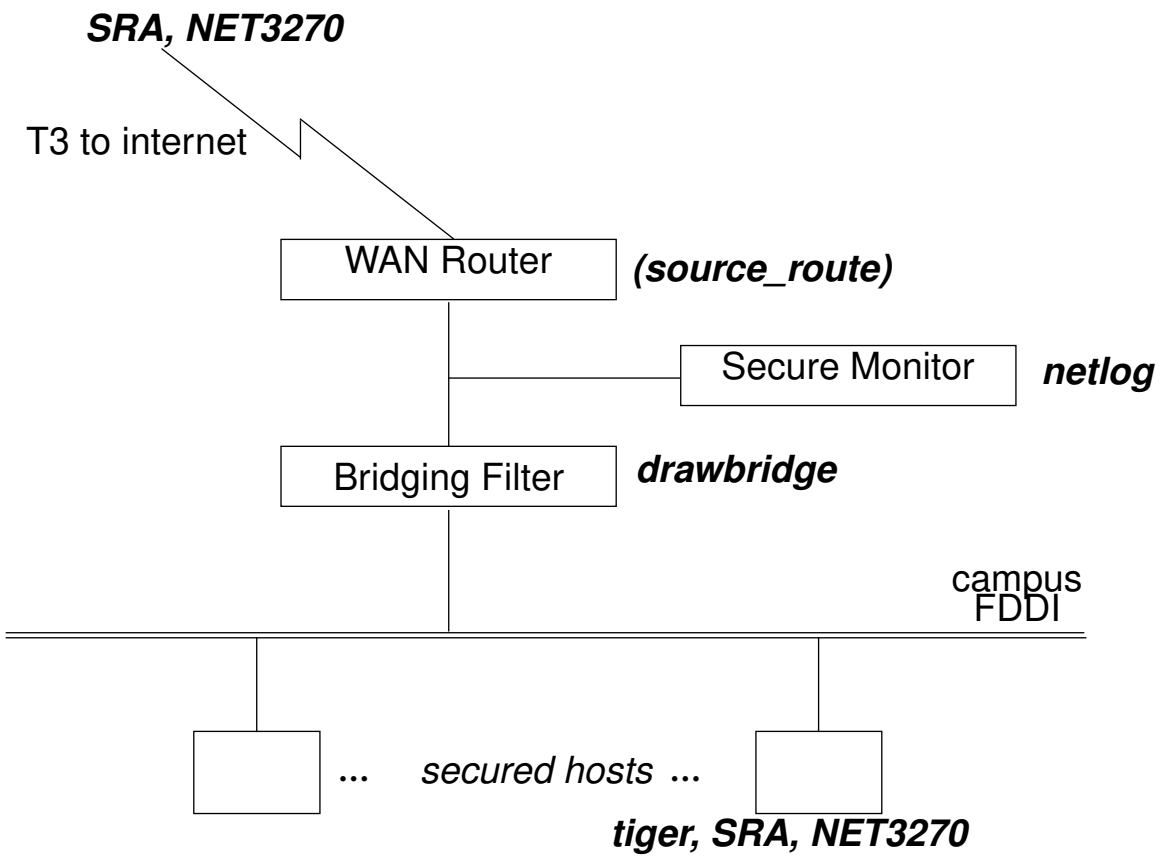
SRA Design

- use unauthenticated diffie-hellman key exchange
- use Sun's Secure RPC code
- telnet and ftp negotiate SRA option

SRA Goals

- Prevent password sniffing
- Drop in replacements for telnet and ftp
  - no external key service
  - portable across platforms
  - compatible with unmodified clients and servers
- avoid RSA patent problems

Overview of Components



Approaches:

- prevent source routing in internet router
- firewall (drawbridge)
- network monitors (netlog)
- host checks (tiger)
- tcpwrapper, s/key
- encryption (SRA, NET3270)
- Passworded Dial-ups, particularly SLIP/PPP
- “Secure” twisted pair ethernet hubs
  (we use 3-COM FMS-2 stackable)
- Backups

NATAS - Dr. David Safford

Texas A&M University

(MAPS)...

History

- 1/91 Taught Graduate Network Security Class
  - cookie, ypfake, xnfs
- 8/92 TAMU Breakins
- 10/93 4th USENIX Security Conference
  - drawbridge, netlog, tiger, SRA
- 11/93 Given responsibility for all Networking
  - FDDI backbone, T3 to internet, Secure 10baseT
- 10/95 Started NATAS

Outline

- History, overview of TAMU tools
- SRA
- NATAS
  - Goals
  - Design
- Comparison to other systems
- Status
- Questions

- Postscript copy of this presentation available from net.tamu.edu:pub/security/TAMU/watson.ps, along with original USENIX article tamu-security-overview.ps, and sra.ps

NATAS - Dr. David Safford

Texas A&M University

Presenter:

Dr. David Safford
Director, Networking and Supercomputing,
Computing and Information Services
Texas A&M University
(d-safford@tamu.edu)

Credits:

David K. Hess
Douglas Lee Schales