SafeTP

Securing File Transfer
Using Transparent Proxies

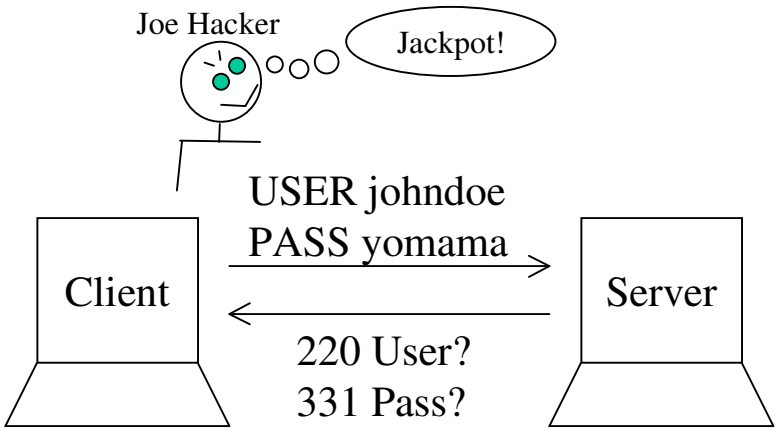
Dan Bonachea

Scott McPeak

UC Berkeley, CS262, Fall 98

The Problem

- FTP Protocol Standard: RFC-959
  - Passwords are sent in the clear:

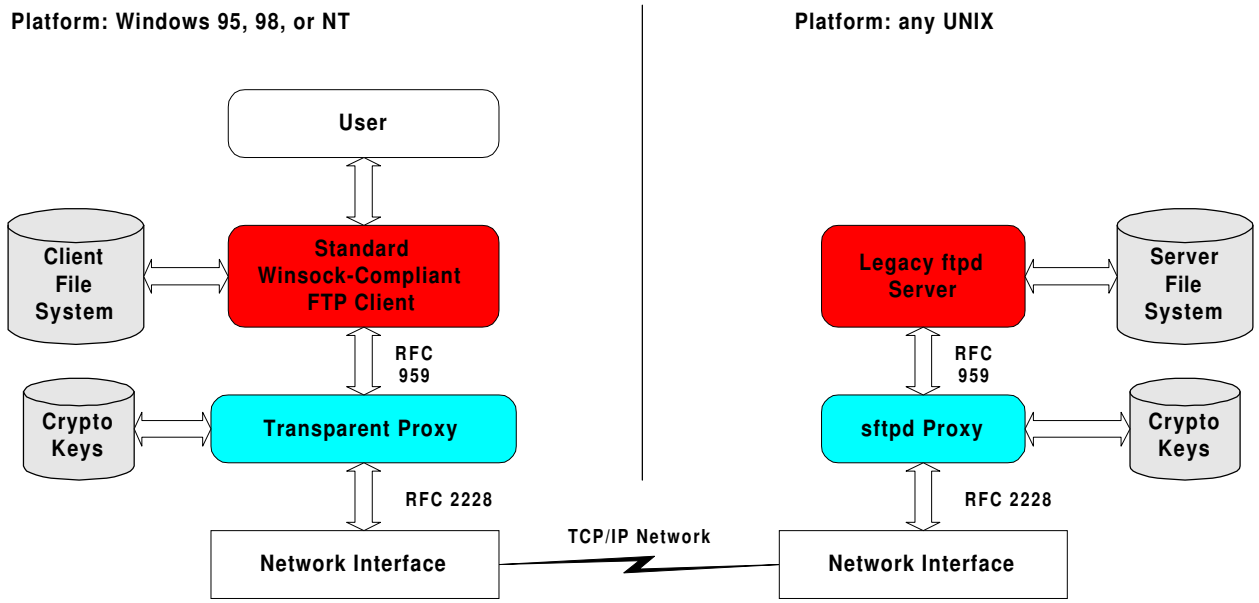


- Deployment Problems
  - Client: New interface means headache for users
  - Server: New daemon means potentially opening new security holes

Our Solution

Transparent Proxies

for both Client and Server

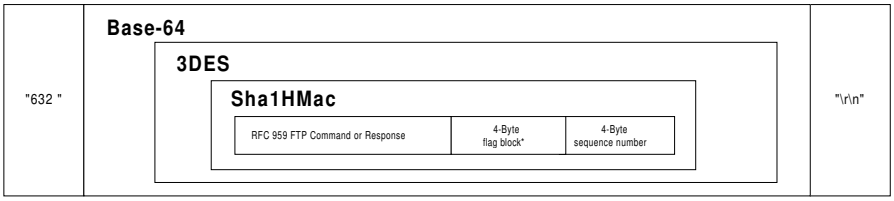


Built-in Interoperability with RFC959-Compliant Clients/Servers

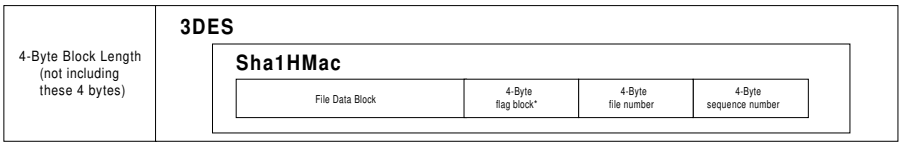
SafeTP Protocol

Adheres to RFC-2228 - “FTP Security Extensions”

Control Block

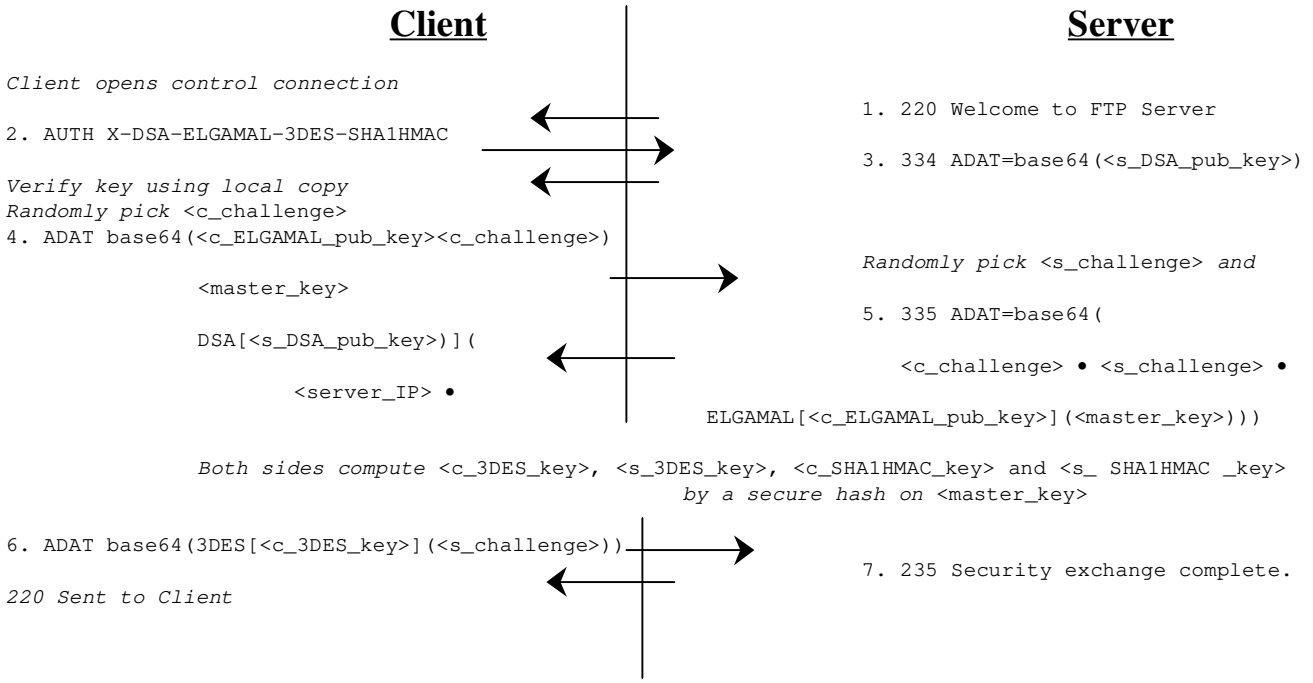


Data Block



Flag Block Detail*

Sample Negotiation



Security Provisions

- Server authentication:
  - Copy of server's DSA public key is stored on the client machine
  - Trust-first-time or obtain through out-of-band methods
- Data protection
  - Privacy: 3DES, ElGamal
  - Integrity Protection: Sha1HMac
- Some attacks we prevent:
  - Packet Replay attacks: sequence numbers,
  - Session Replay attacks: per-session challenge/response
  - Packet sniffing
  - Playing router
  - Complicated redirection attack
  - 959 attack

Code Extensibility

Designed to easily incorporate new security mechanisms in the future

Interface:

```
class Transform {
    virtual int maximumEncodedSize(int decodedSize) const=0;
    virtual int maximumDecodedSize(int encodedSize) const=0;
    virtual void encode(DataBlock &data)=0;
    virtual void decode(DataBlock &data)=0;
    }
```

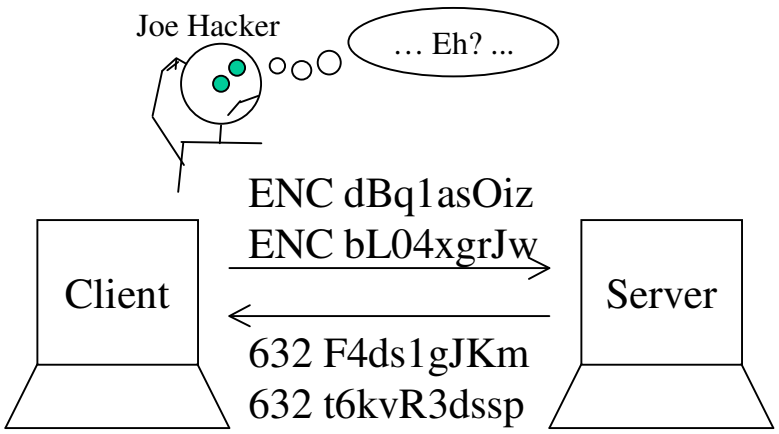
```
class ControlSecurity{
    virtual bool hasOutgoingAdat() const;
    virtual void getNextOutgoingAdat(DataBlock &block);
    virtual bool expectingIncomingAdat() const;
    virtual void incomingAdat(DataBlock &block);
    }
```

Deployability

- Client (SafeTP):
  - Proxy runs on Windows 95/98/NT
  - 2-minute, no-hassle installation,
    then you never need think about it again
  - Uses Winsock 2.0 SPI interface

- Server (sftpd):
  - Install on port 21, move legacy ftpd to new port
  - Always runs as “sftpd” user, who only has permissions to his home directory

- Both Client and Server:
  - Built-in interoperability with RFC-959 protocol

Contributions

- Secures FTP password
- Option to secure data transfers
- Easily deployed
- First implementation of the RFC-2228 standard that we know of