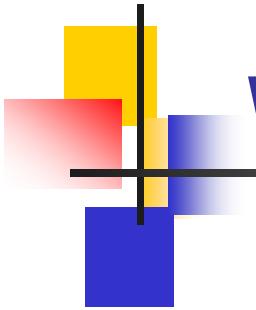
A high grade secure VoIP using the TEA Encryption Algorithm

By

Ashraf D. Elbayoumy

2005 International Symposium on Advanced Radio Technologies

Boulder, Colorado
March 1, 2005

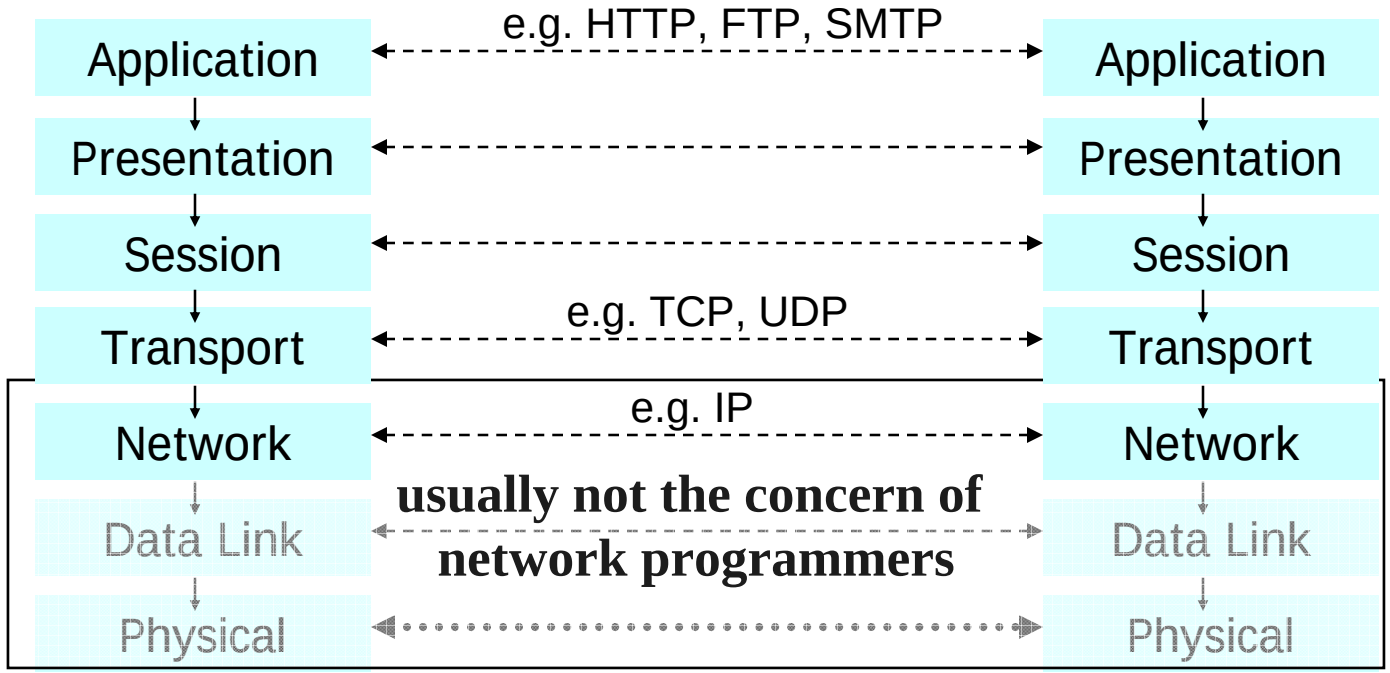


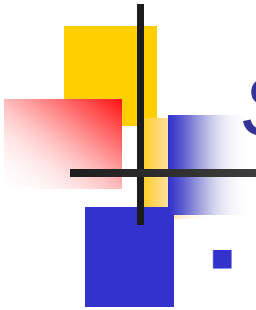
Voice over IP (VoIP)

In recent years, we have witnessed a growing interest in the transmission of voice using the packet-based protocols. Voice over Internet protocol (VoIP) is a rapidly growing technology that enables the transport of voice over data networks such as the public Internet.

About Network Programming

- networks are organized as a series of layers (or levels)
- the rules to communicate are called protocol
- Examples of protocol: TCP, UDP, IP, Ethernet, HTTP
- the OSI reference model defines seven layers:

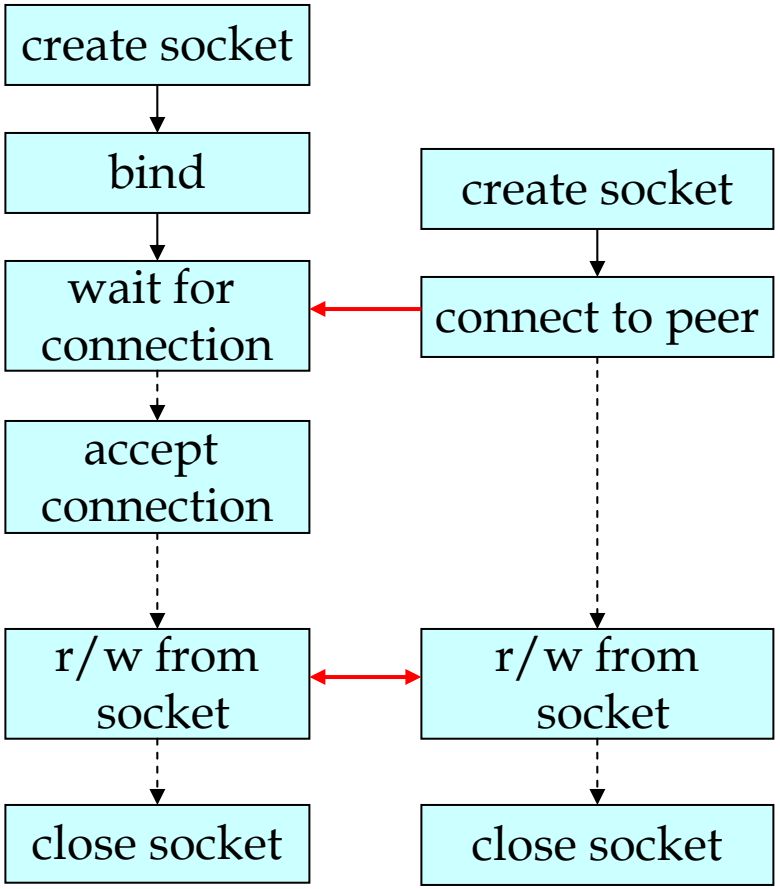




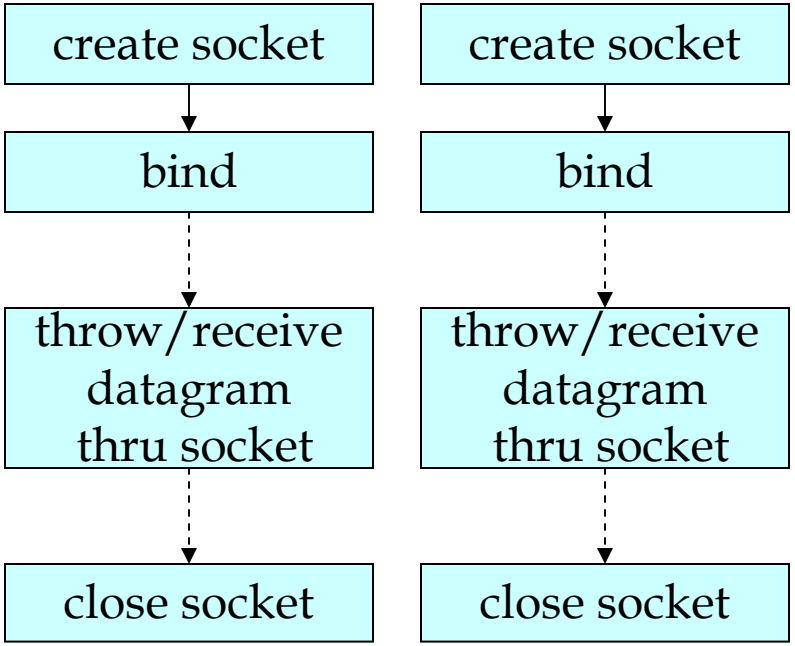
Socket

- Socket is the endpoints of a communication channel
- In Unix, the standard is BSD socket; in Windows, we use WinSock.
- WinSock basically follows the BSD socket standard, but there are some modifications.
- The latest version, Winsock 2, provides more support for various protocols.
- Two types of sockets
  - SOCK_STREAM (TCP)
  - SOCK_DGRAM (UDP)
- TCP is connection-oriented, reliable, … A stream socket works much like an input/output stream.
- UDP is connectionless, unreliable, send and receive in packets (may arrive out-of-order)

Typical Work Flow

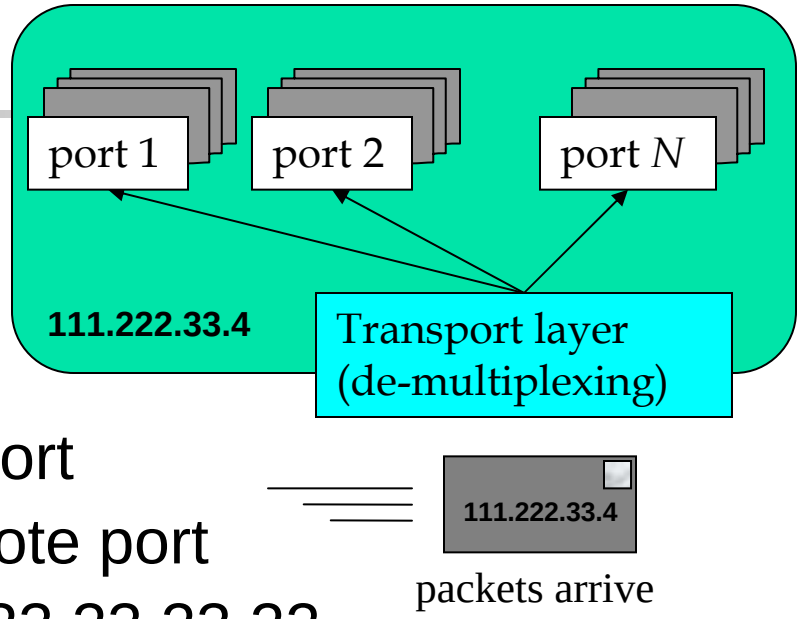


connection-oriented
(SOCK_STREAM, TCP)

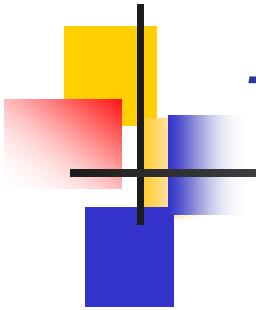


connectionless
(SOCK_DGRAM, UDP)

Programming Basics



- Things to fill in:
  - protocol
  - local IP address, local port
  - remote IP address, remote port
- IP address is in the form 123.23.23.22
- Choose a port:
  - some well known ports
  - for network programming, choose port number > 1024



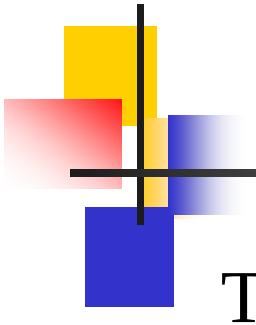
The basic idea behind VoIP

The user's voice is converted from analogue form into a digital form, compressed and broken down into a series of packets (Packetisation). These packets are then routed through private or public IP networks from one user to another and reassembled and decompressed at the receiving side.

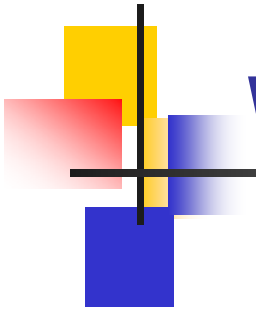
Quality of Service is fundamental to the operation of a VoIP network. Despite all the money VoIP can save users and the network elegance it provides, if it cannot deliver at least the same quality of call setup and voice relay functionality and voice quality as a traditional telephone network, then it will provide little added value.

Among the factors that degrade voice quality are end-to-end delay, packet loss, delay variation, or jitter, voice compression schemes (CODECs), echo cancellation algorithms.

In the case of voice transmission, the maximum acceptable delay in packet delivery for optimal voice quality is 150ms, which can be extended up to 200ms in case of encrypted communications.



The time spent by the CODEC, the device that performs the digitization process, may vary between 0.75-30ms, depending on the coding schemes adopted and the quality of the reproduced signal. The queuing delay (i.e., the time spent by a packet in the router buffers waiting for being routed) may add up to 30 ms. A further delay in the range of 40-70ms, called jitter delay, is introduced by buffering arriving packets so that they can be delivered at a uniform rate.



VoIP Security

Security is a serious bottleneck for the future of VoIP (anyone with physical access to the office LAN can potentially connect network-monitoring tools and tap into telephone conversations) . Because of the time-critical nature of VoIP most of the same security measures currently implemented in today's data networks could not be used in VoIP networks.

VoIP Security Vulnerabilities

- **Voice transport protocols**
  - *RTP*
  - *RTCP*
  - *SCTP*
  - **Signaling protocols and architecture**
  - *SIP*
  - *H.323*
  - *MEGACO*
  - *MGCP*

What's at Risk?

- IP phones
- Core routers
- Media gateways
- SIP proxies
- Gatekeepers
- Location servers
- Switches
- VoIP-based firewalls
- Any equipment in VoIP infrastructure

Voice Data Convergence Multiplies Threats

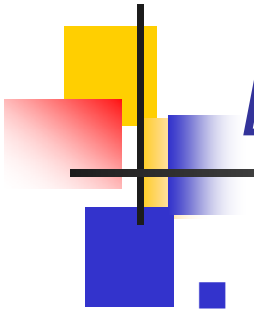
- **VoIP inherits IP data network threat models**
- *Reconnaissance, DoS, host vulnerability exploit, surveillance,*
- *hijacking, identity theft, misuse, etc.*
- **VoIP QoS requirements increase exposure to DoS**
- **attacks that affect:**
- *Delay, jitter, packet loss, bandwidth*
- **PCs = authentication; phones = any user**
- **User identity theft**
- *VoIP inherits PBX phone vulnerability*
- *Unauthorized access and privileges, service theft*
- **Device identity theft**
- *Malicious devices on IP network act like IP phones*
- *Reduced service availability, eavesdropping*
- *Inserting/Deleting/Modifying audio streams*

Threats from Phreakers and Hackers

- **Phreakers use phone system to:**
  - *Gain free calls*
  - *Disrupt system*
  - *Fun*
  - **Hackers use computer system to:**
  - *Gain free services/products*
  - *Denial of Service (DoS)*
  - *Business*
  - *Fun*

Denial of Service Threat

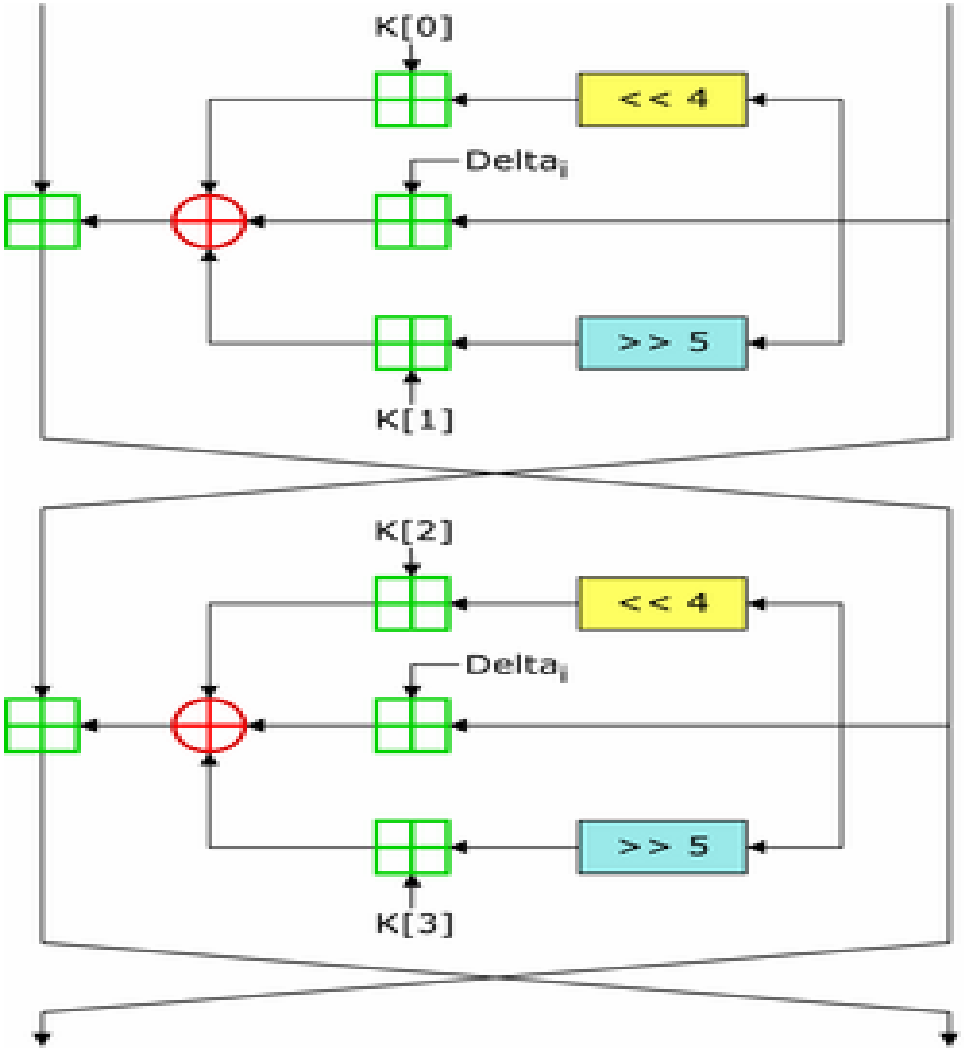
- **DoS venues**
- *Flood*
- *Abuse protocols*
- **Target devices**
- *IP phones (easy)*
- *Routers, switches (depends on equipment)*
- *Signaling gateways, media gateways, SIP proxies*
- *Any device in the path a call takes from a caller to a*
- *called party*

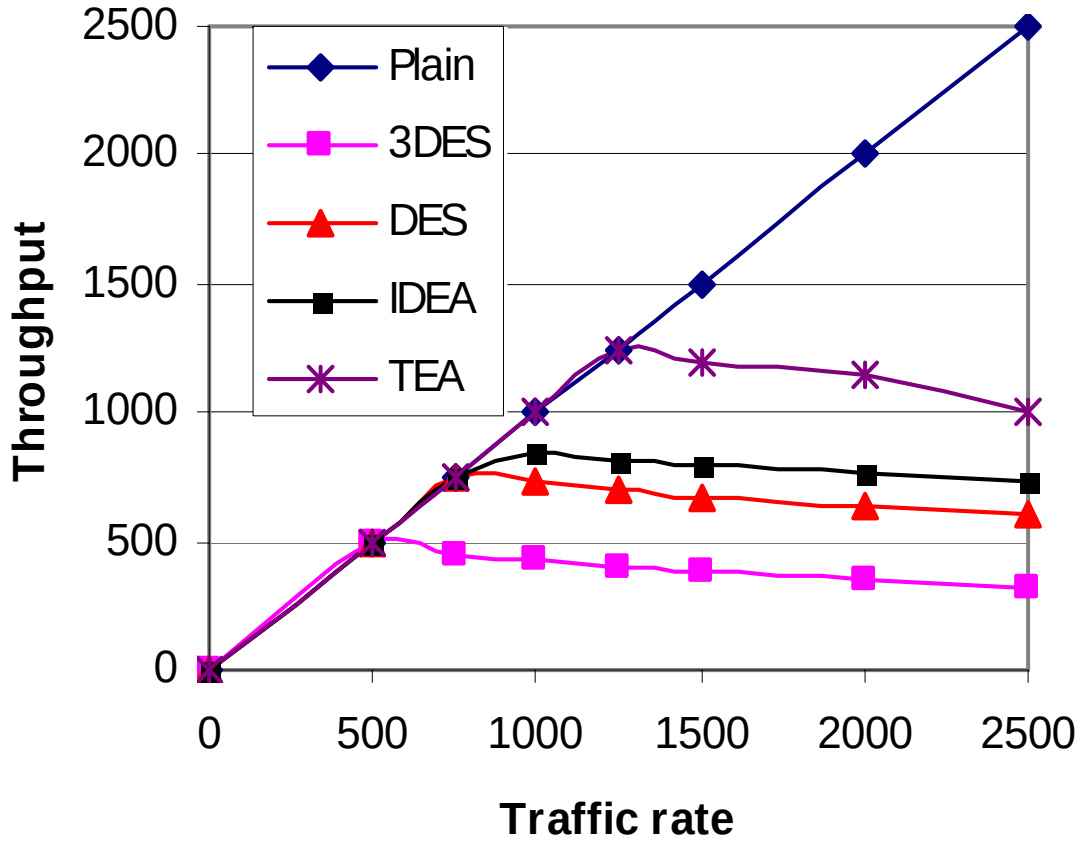


Encryption Algorithms:

- DES
- 3DES
- IDEA
- BLOWFISH
- TEA

Two rounds of the TEA block cipher




2500
2000
1500
1000
500
0
Throughput
Plain
3DES
DES
IDEA
TEA
0
500
1000
1500
2000
2500
Traffic rate

Thank You