Internet Security – Stakeholders, Issues, and Examples

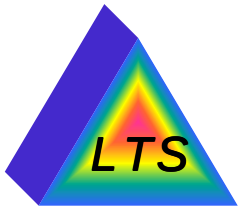
Gary Hayward
Telcordia Technologies and
Laboratory for Telecommunications Sciences
gah@research.telcordia.com
301 688 1729
May 13, 2002

An SAIC Company

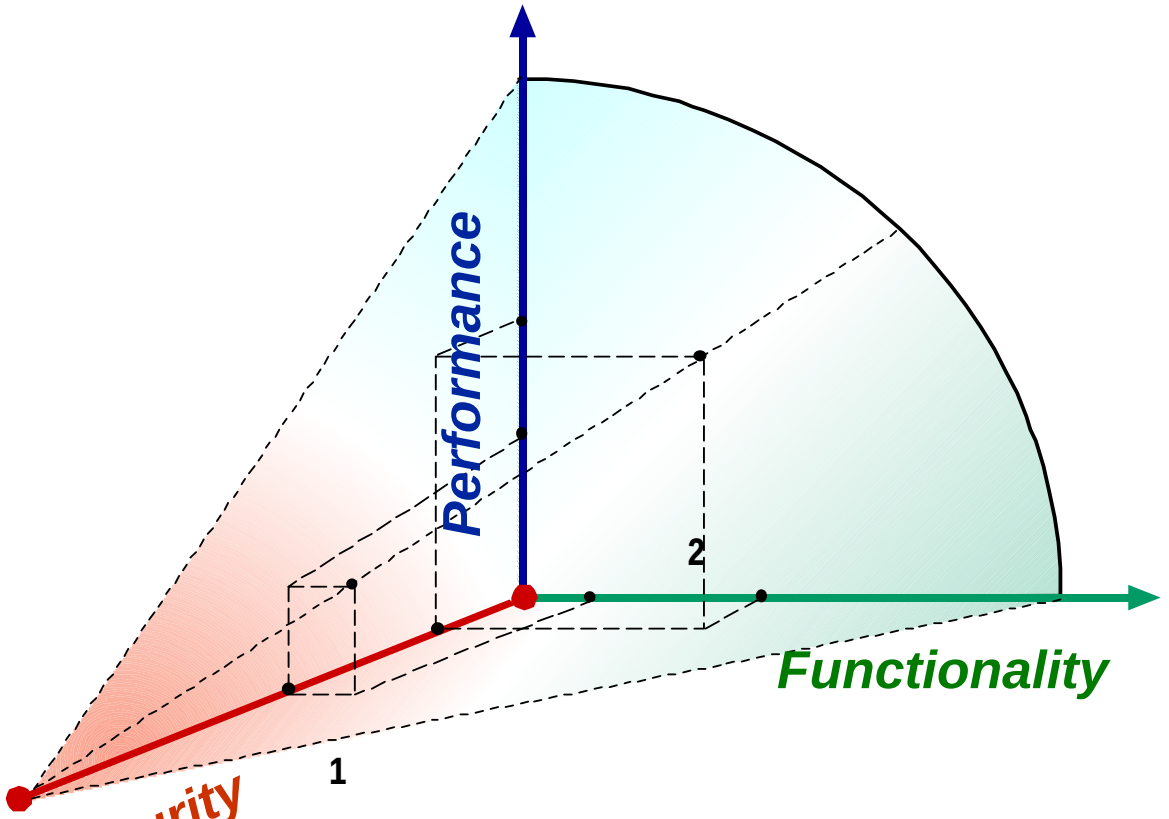
Outline

- Goals in internetwork security and service assurance
- Five stakeholder classes
- Illustrative Examples
  - Using Secure Socket Layer (SSL) to protect a TCP session
  - Using multiple security technologies to support telecommuting
- Paradoxes in network security for the next generation

Telcordia Technologies
Performance from Experience



The Information Assurance Challenge



Confidentiality, Integrity, and Availability

Sami Saydjari, DARPA Information Assurance Program, January 2001

Telcordia Technologies
Performance from Experience

LTS

Five Network Security Stakeholder Classes

- Engineering
  - Applying what we know how to do in network security
  - Scaling it up to global dimensions
- Research
  - Exploring what we don't know how to do in network security
  - Finding the the science amidst the issues
- Education
  - Building a basis of network security professionals
  - Finding fresh ideas and documenting old failures
- Business
  - Selling the next thing we learn how to do in network security
- Law and Public Policy
  - Distributing the network security burdens and resources

Telcordia Technologies
Performance from Experience

LTS

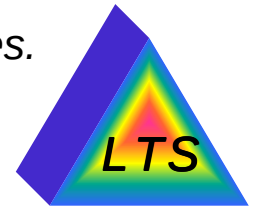
Engineering

- Enterprise Firewalls
- Secure Web Servers and Services
- Virus Checkers
- Intrusion Detection
- Anomaly Detection
- Authentication, Authorization, and Accounting
- Virtual Private Networking
- Insider Misuse Detection
- Cryptographic Transforms and Certificates

- Scaling up to larger infrastructures
- Reducing event response times

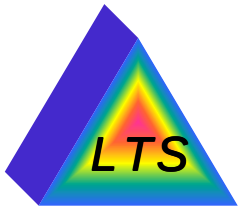
Much of Security Engineering consists of "check box" deployment of functions and services deemed appropriate to corporate Best Practices.

Telcordia Technologies
Performance from Experience



Research – Enduring Hard Topics

- Composition – assembling low assurance components into high assurance systems
- Dynamic Coalition of separately administered networks and software systems
- Dynamic policies which adapt to a changing environment
- Network perimeter mapping
- Integrated software quality control with global outsourcing of development
- Information Filters and Enclave Boundary Controllers
- Large network recovery – what to do with a network 50% degraded?
- Global network forensics and supporting legal processes
- Matching access controls to legitimate workflows
- Metrics of success, vulnerability, and return on investment



Education

- Finding fresh ideas without rediscovering old poorly documented failings
- Founding the science and methodology of network security
- We have good cryptographic capabilities, where is the rest of our practice?
- Extension of computer security science from Unix workstations to embedded global communications systems.
- Building the aggregate knowledge base of defenses and hacks.
- Integrating network security and service assurance into business management curricula
- Integrating network security and service assurance into international law and public policy curricula

Telcordia Technologies
Performance from Experience

LTS

Business

- Where is the return on investment for network security?
- How do we shift liability for insecure systems away from our enterprise?
- Where is the actuarial data for cyber insurance?
- If you grow fast enough, you may self-insure more cheaply than secure – even become too big to fail

- Securing the Network adds cost
- Security delays limit market entry
- Many new worries, little new funding
- Many business failures, few due to faulty security

Telcordia Technol

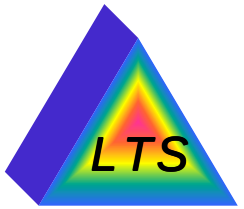
Performance from Experience

LTS

Law and Public Policy

- What is the distribution of responsibility and liability in a global network?
- What responsibilities would ~6 dominant global communications service providers and ~200 national governments owe one another?
- Does network security come under contract/tort law, Common Carrier regulation, or international treaties?
- What are the transitive liabilities of Universities and enterprises used as Denial of Service Zombies and attack amplifiers?

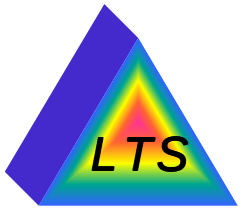
Telcordia Technologies
Performance from Experience



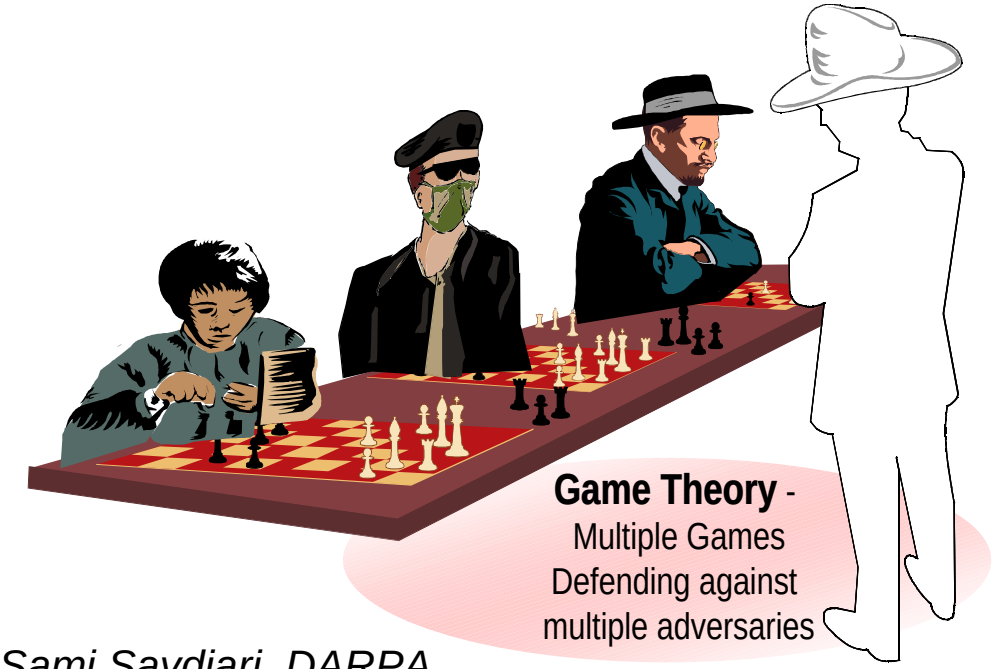
Some Classes of Adversary

- Fraud
  - Seeks money
- Hacktivist
  - Seeks publicity and demonstration of vulnerability
- Recreational Cracker
  - Seeks superiority and challenge
- Internal Misuse
  - Seeks anything from Web surfing on company time to malicious attack
- National and transnational attack
  - Seeks Demonstration of strength, paralysis of infrastructure, …

Telcordia Technologies
Performance from Experience



One Defense Against Multiple Adversaries



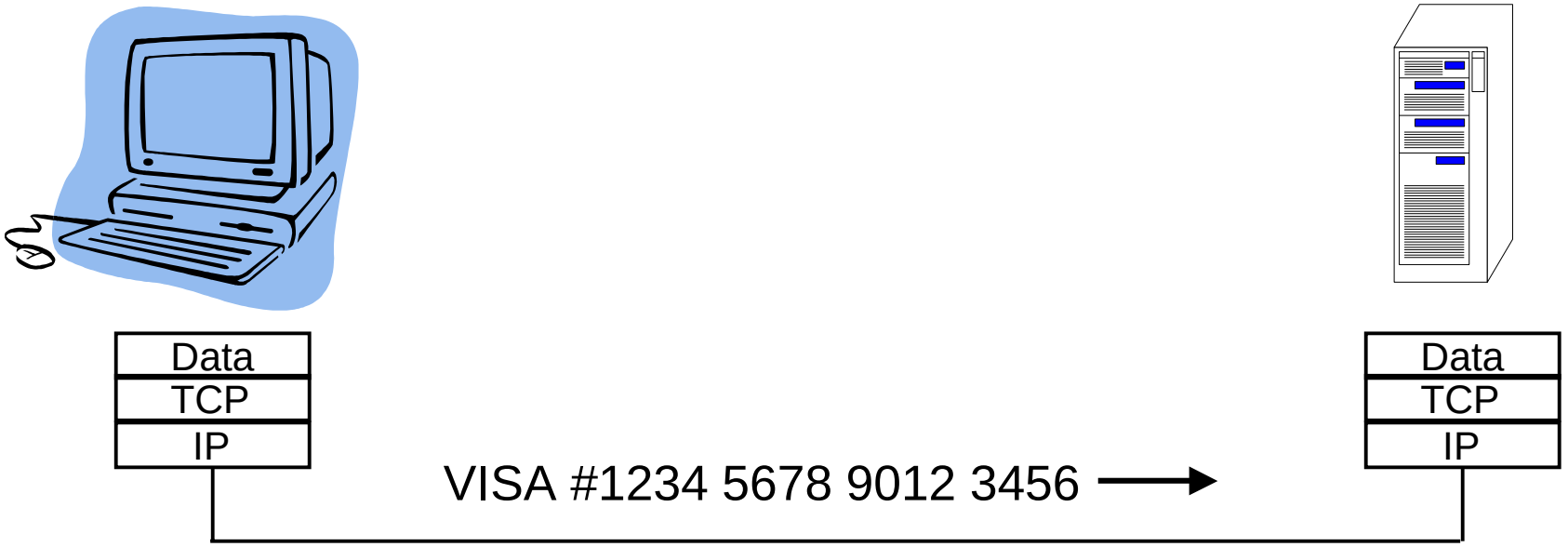
Sami Saydjari, DARPA Information Assurance Program, January 2001

The defender gets one set of pieces to defend against multiple diverse threats.

Telcordia Technologies
Performance from Experience

LTS

Example – SSL Web Commerce

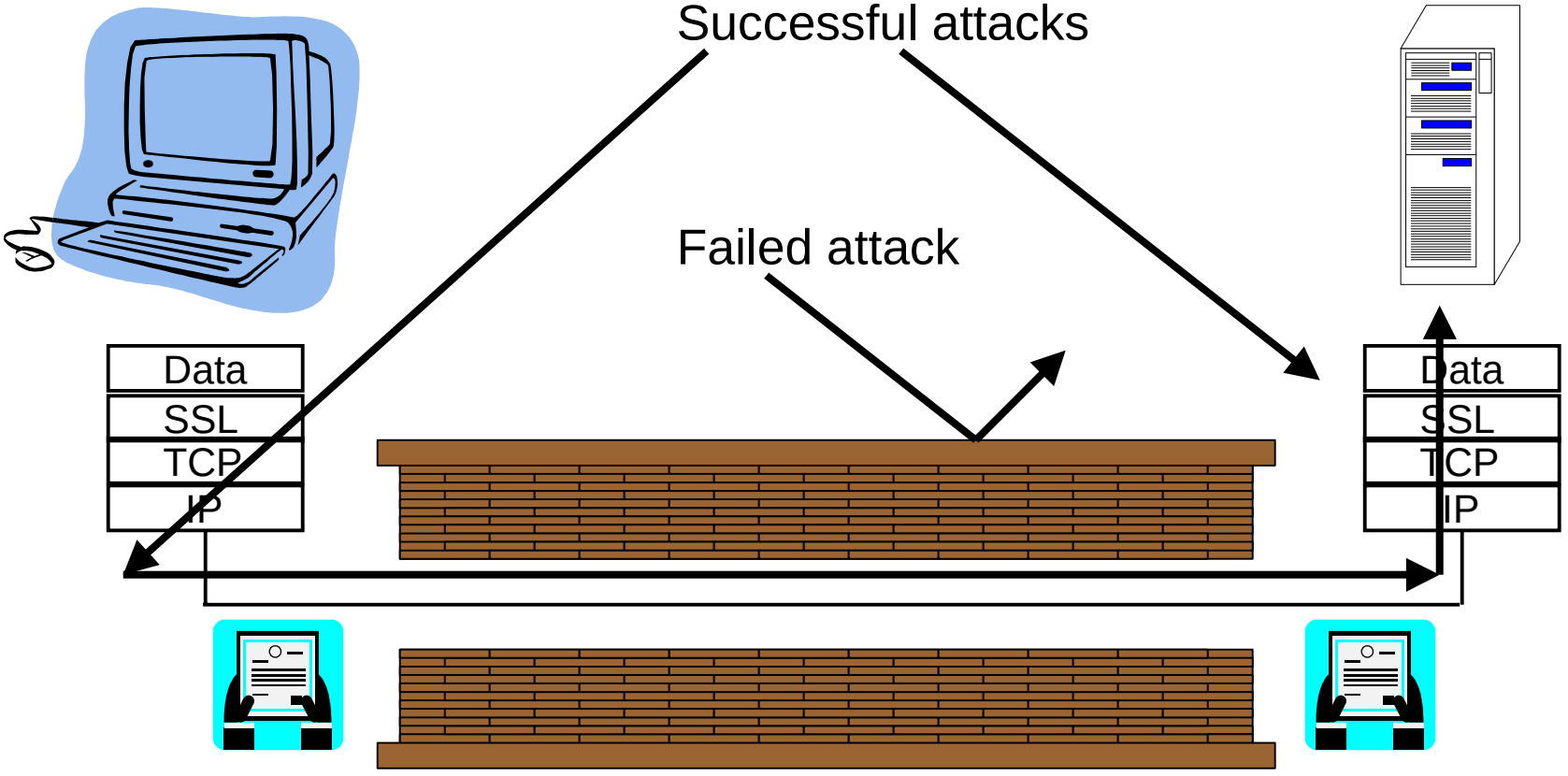


An HTTP Insecure Web Session

Telcordia Technologies
Performance from Experience

LTS

Example – SSL Web Commerce



An HTTPS Secure Web Session

Telcordia Technologies
Performance from Experience

LTS

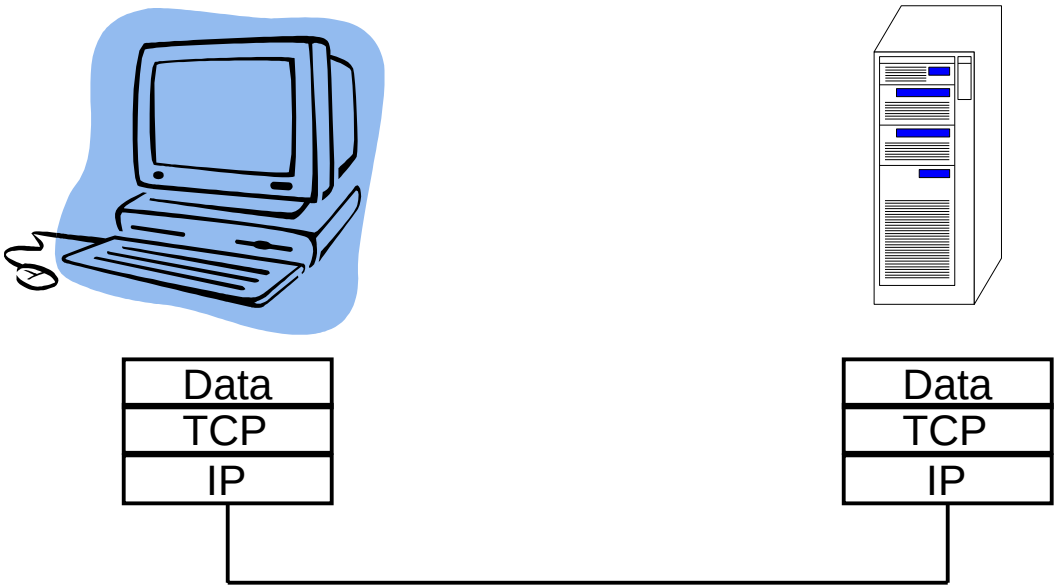
Example – Telecommuting over a VPN

- The Scenario
  - Government mandates an emergency transition from automotive commuting to telecommuting – how do Commercial, Educational, and Government agencies extend secure Virtual Private Networks to residences, enterprise hotels, and regional access points?
  - Consider a residence with two ex-commuting employees and two children sharing a single wireless LAN
    - Map out the VPN protocols needed to keep commerce running

Telcordia Technologies
Performance from Experience

LTS

Telnet without Added Security
appropriate to an Enterprise Intranet

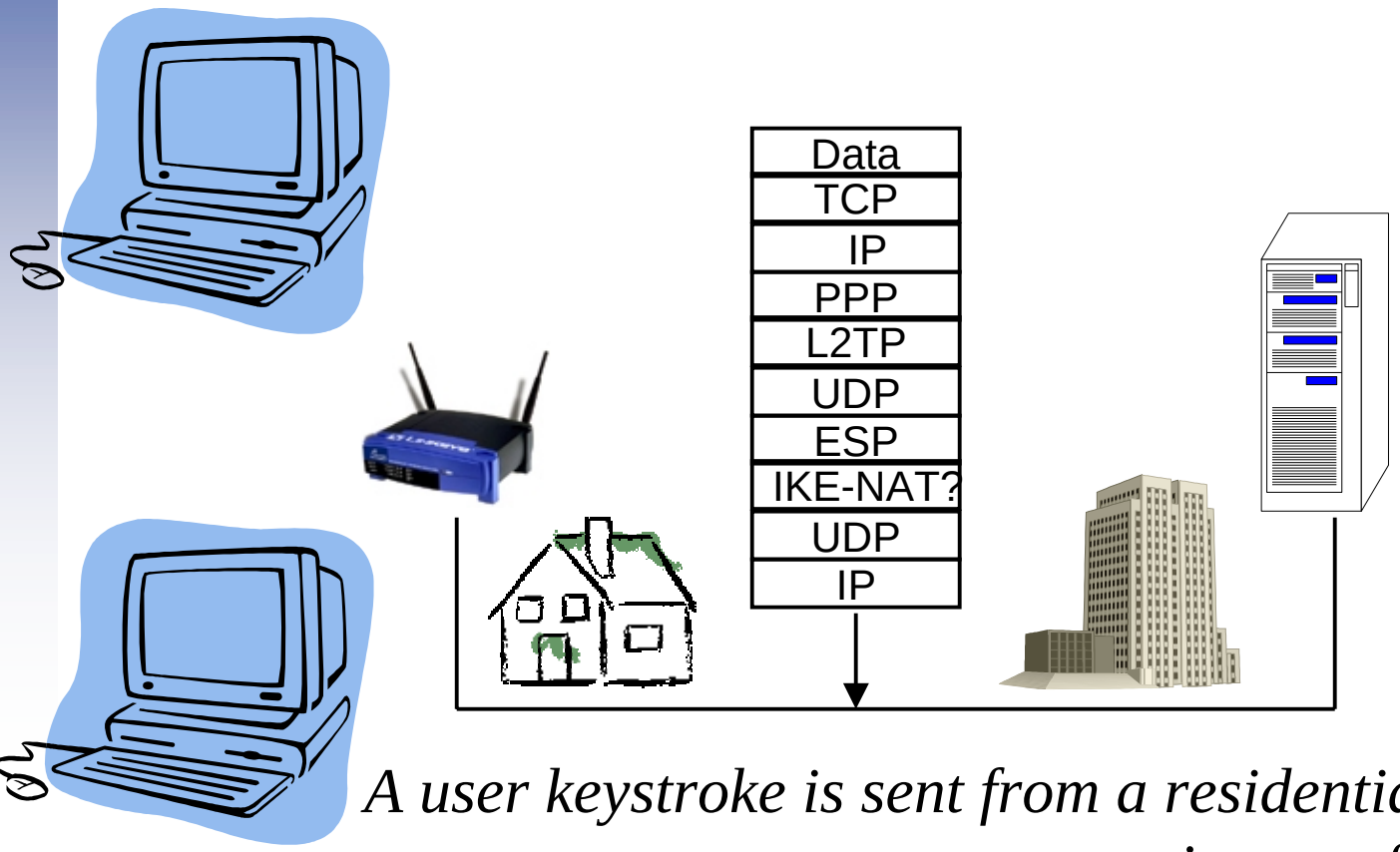


A user keystroke is sent to a server

Telcordia Technologies
Performance from Experience

LTS

Telnet with VPN Security

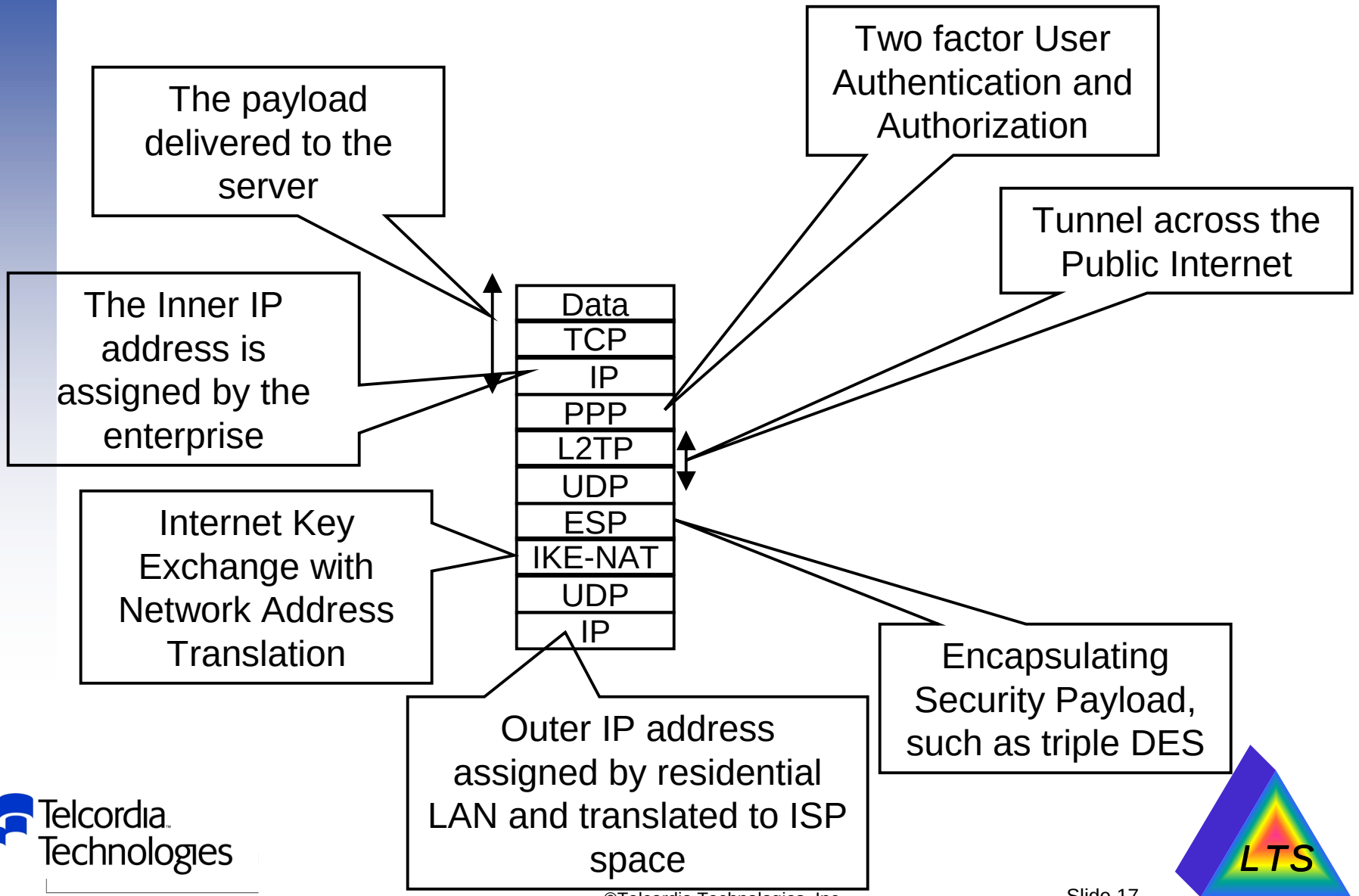


A user keystroke is sent from a residential computer to a corporate server in one of several possible VPN layerings

Telcordia Technologies
Performance from Experience

LTS

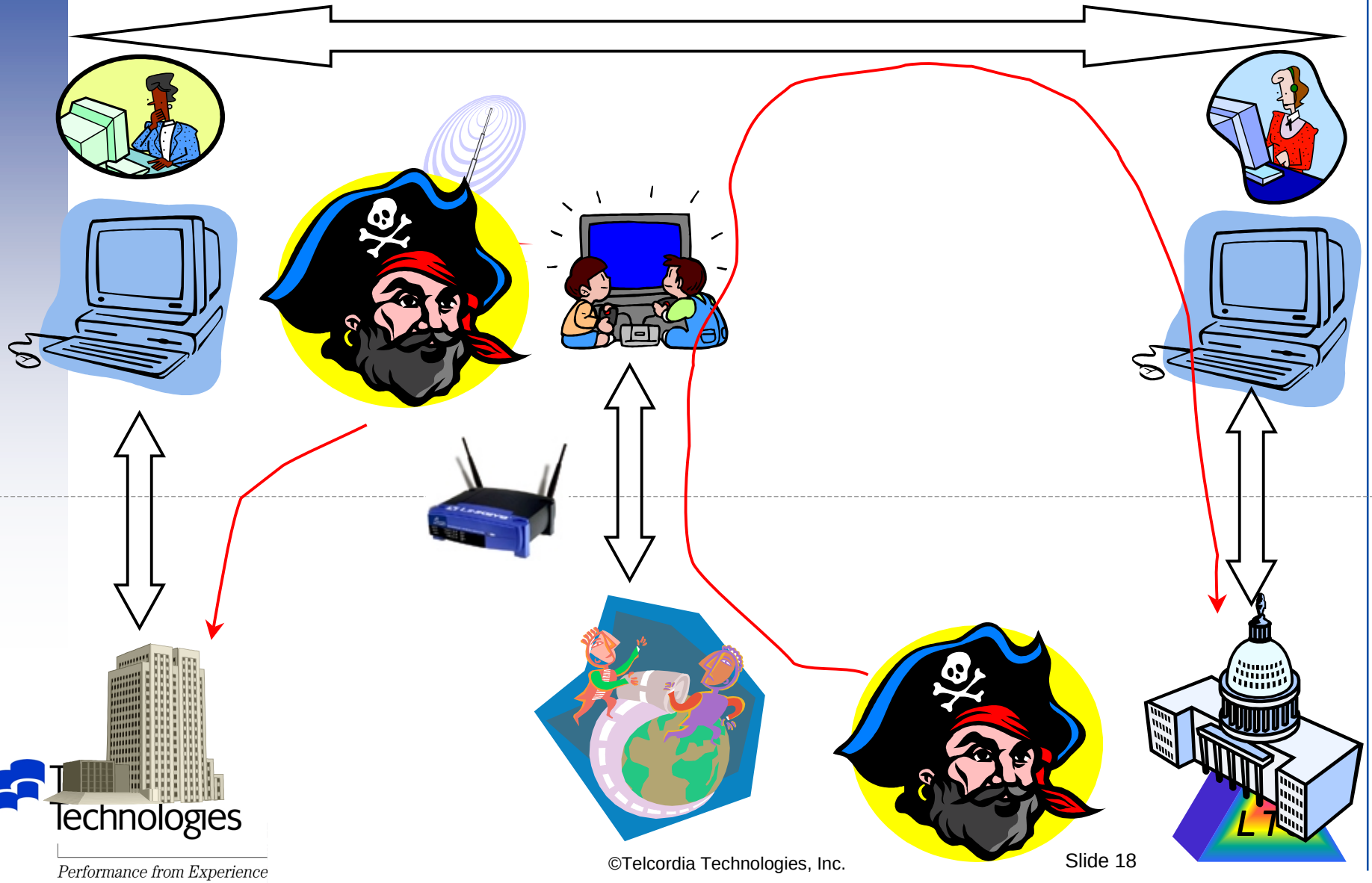
Security Layering



Telcordia Technologies
Performance from Experience

LTS

Sharing the Telecommuters' Residential Wireless LAN



Technologies

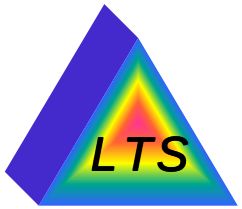
Performance from Experience

A Cable Modem Service Agreement

i. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, THE SERVICE IS FOR PERSONAL AND NON-COMMERCIAL USE ONLY AND CUSTOMER AGREES NOT TO USE THE SERVICE FOR OPERATION AS AN INTERNET SERVICE PROVIDER, A SERVER SITE FOR FTP, TELNET, RLOGIN, E-MAIL HOSTING, "WEB HOSTING" OR OTHER SIMILAR APPLICATIONS, FOR ANY BUSINESS ENTERPRISE, **OR AS AN END-POINT ON A NON-[Service provider] LOCAL AREA NETWORK OR WIDE AREA NETWORK, OR IN CONJUNCTION WITH A VPN (VIRTUAL PRIVATE NETWORK) OR A VPN TUNNELING PROTOCOL;**

Added security may be a contract violation without paying your ISP an increased fee!

Telcordia Technologies
Performance from Experience



Assurance Paradoxes to Refute

- Any given incremental defender's effort can be bypassed by a smaller adversary effort
- Any comprehensive network is too complex for a single defender to partition, map, or systematically protect
- The incremental deployment of 3-DES adds unauditable connectivity which decreases security
- Anomaly detection gear is, for some threats, provably worse than random guessing
- For a corporation to discuss a network security problem in public is to become liable for its solution
- The "Denial of Service Server" – new security solutions are attractive and fragile targets

Telcordia Technologies
Performance from Experience