

Security & Safety Issues in Next Generation Telemedicine Design

For The
American Telemedicine Association Annual Meeting
May 22, 2000

Rick Craft
Sandia National Laboratories
505-844-8873 rlcraft@sandia.gov



Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin company, for the United States Department of Energy under contract DE-AC04-94AL85000.



Our Original Problem

Physician Station



Patient Station



Identify &
Authenticate
Doctor &
Patient

Control Access to
Patient Records

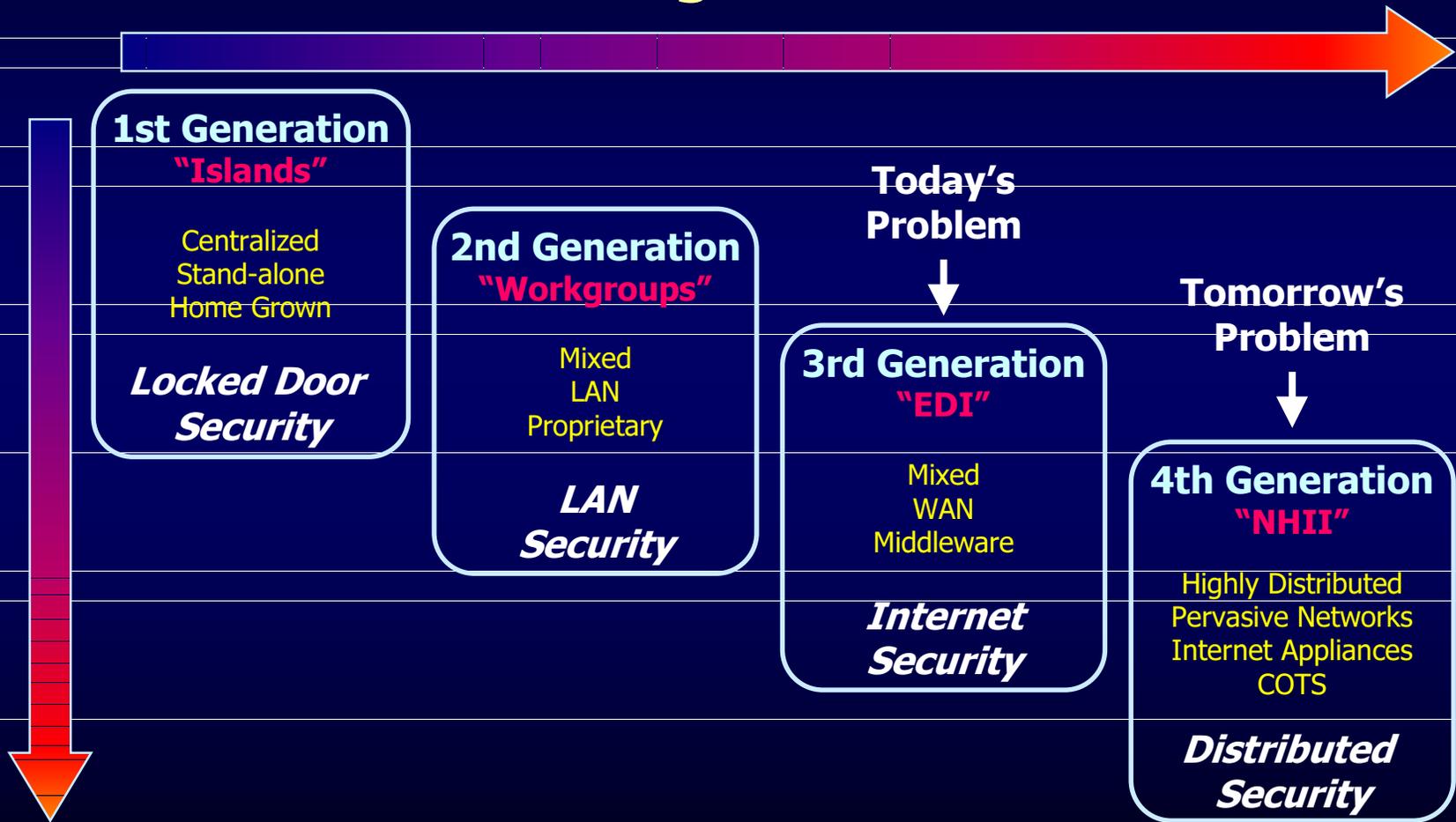
Mark Data to Guard
Against Replay Attacks
& Encrypt Marked Data



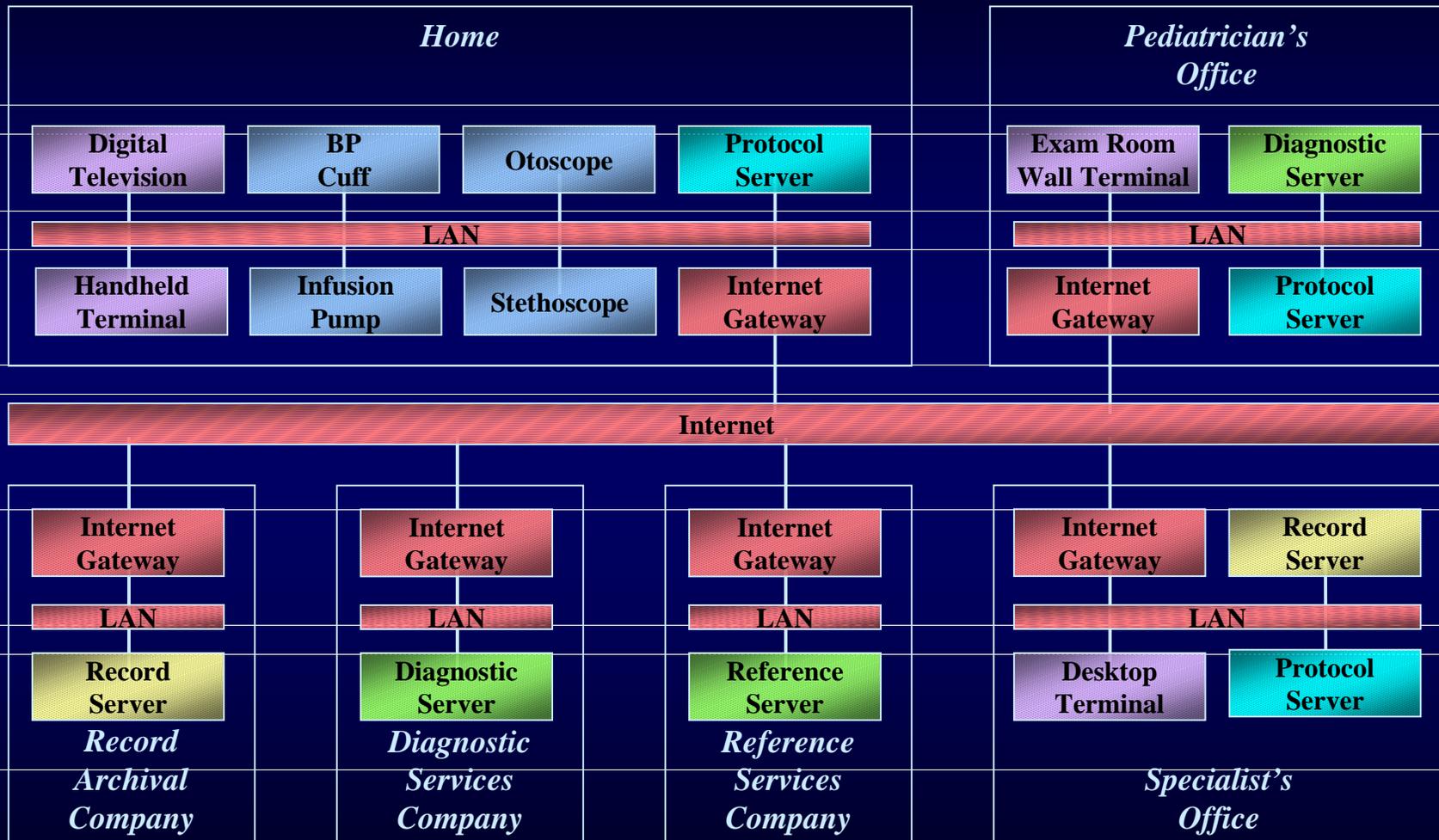
Evolution of Medical Information Systems

Integration

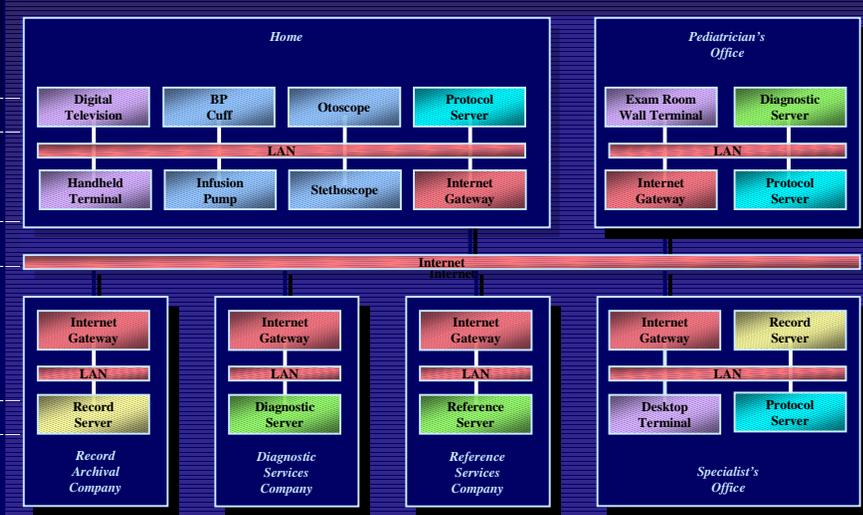
Distribution



A Distributed Telemedicine System

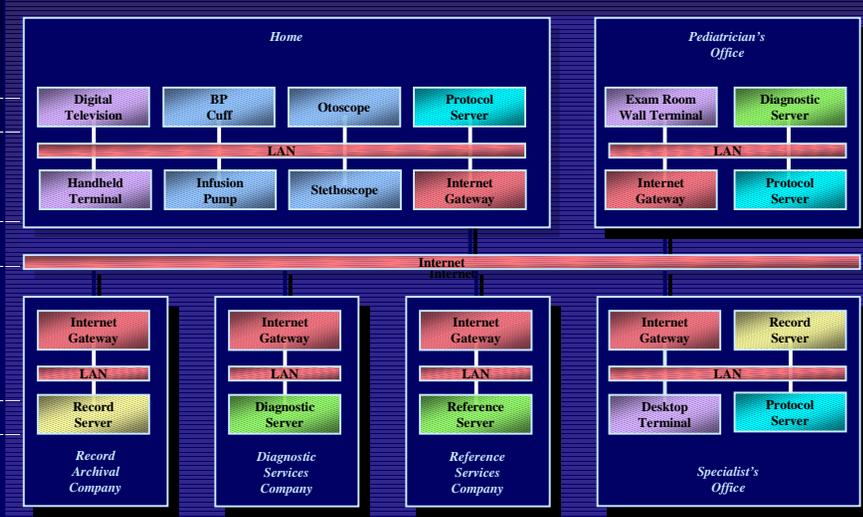


Telemedicine Has Some "Old" Requirements ...



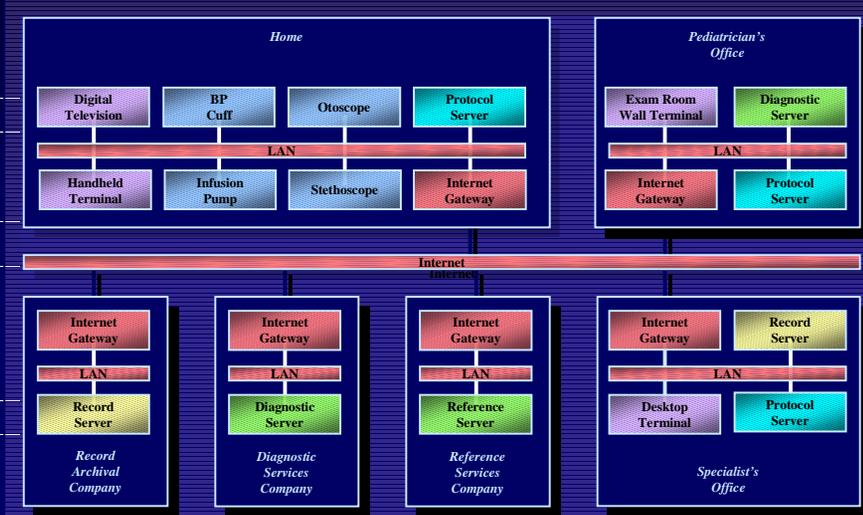
- User identification and authentication
- Authentication and encryption of data
- Control of access to information and methods
- Intrusion detection and auditing
- Quality of service mechanisms

Some "New" Requirements ...



- Trust policy negotiation
- Certification of service providers
- Mobile code assurance
- Dynamically configurable security mechanisms
- Assurance of clinical agents
- "Device" safety in systems composed of pieces developed by independent vendors

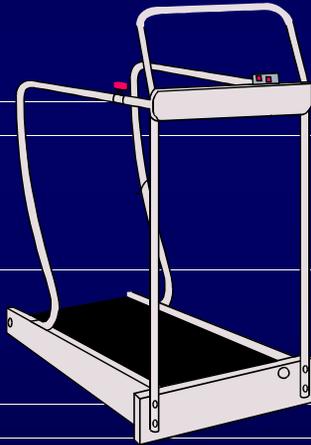
And Some Unique Constraints



- Extreme decentralization
- Ultra-large scale
- Use of clinical devices and services by non-clinicians
- Administration of system by non-experts
- Proliferation of "medical software"

Thoughts On How To Do This

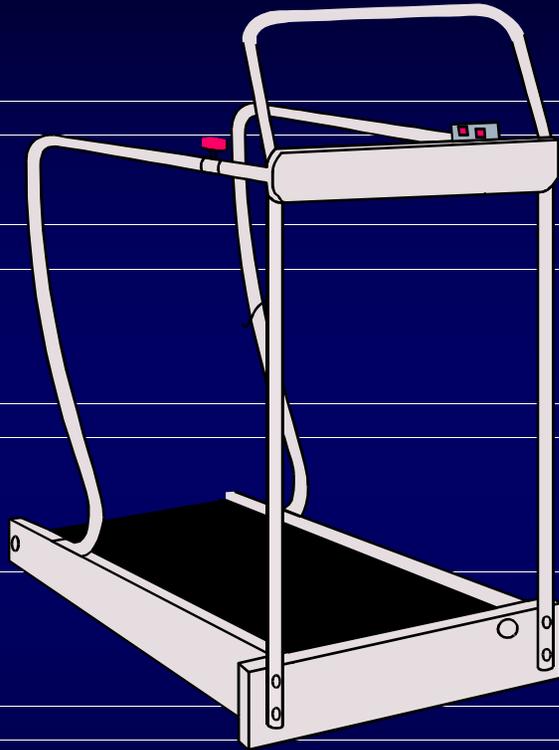
Devices with fixed security features



Devices with variable security features



Device With Fixed Security Features



- End node can be vested with significant capabilities
- “Aware” of its own security capabilities
- Advertises these capabilities during establishment of sessions
- Adding to a system for the first time may result in system reconfiguration to accommodate features introduced by the device

Device With Variable Security Features



- Can explore capabilities of nodes with which it wishes to federate
- Negotiates policy with other variable feature nodes
- Adapts its operation as needed to accommodate fixed feature nodes

An Example

