A Keystone Contribution

Lucent Technologies
Bell Labs Innovations

1876
The Telephone

1939
1st Digital Computer

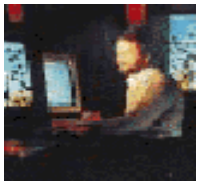
1947
The Transistor

1958
The Laser

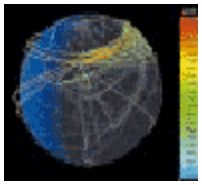
1962
The Telstar Satellite

1969
Unix

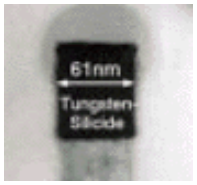
1988
Digital Cellular



1989
HDTV



1995
Data Mining &
Visualization

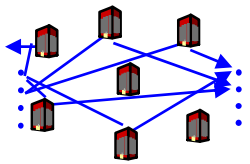


1997
World's Smallest
Transistor

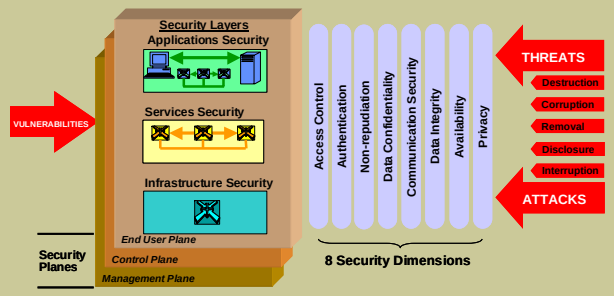
1998
Wide Bandwidth
Optical Amp

1999
All Optical
Router

2000
3.28Tbps
Transmission



2002
BLAST (MIMO)
Hi- Capacity RF



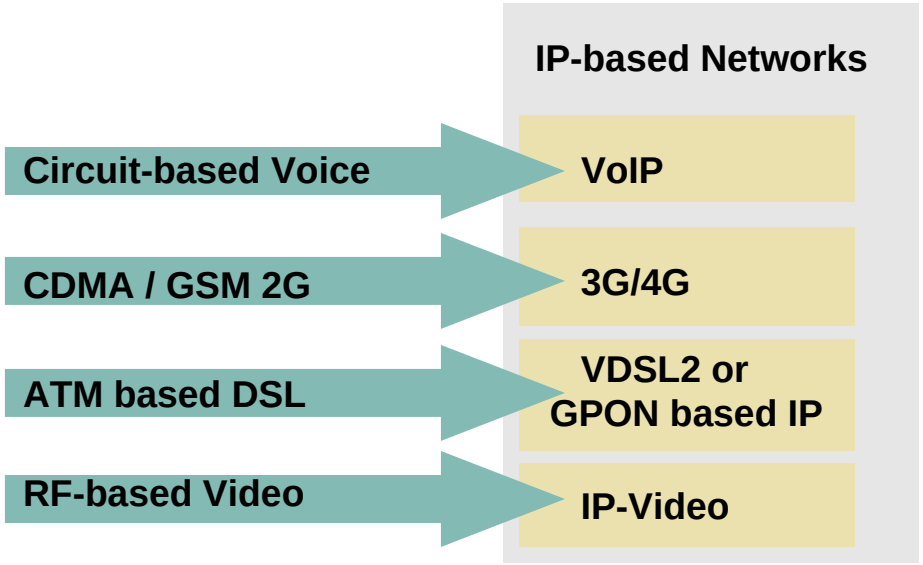
2003

End-to-End Network Security Reference Architecture Foundation of new ITU X.805 specification

The Value of ….”built on standards”

- Trust Based Computing must begin with a trusted platform
- The Bell Labs Security Framework scales from the component to the enterprise and the infrastructure
- In combination with other standards – a comprehensive, in depth security framework for the network and the organization
- We cannot solve the challenges of security without a standard approach
- Improve common criteria – to give it definition at a granular level and improve efficiency in product design and assessments
- Improve FISMA – a specification based view of security that is clear and unambiguous….remove subjectivity – add clarity to the state of security

More Urgent Than Ever…



The Upside…

- Fewer Layers / Less Cost
- Large Supply of Components
- Enhanced Integration Potential
- Improved Bandwidth Management / QoS
- Capture Meta-Data to Use in Marketing

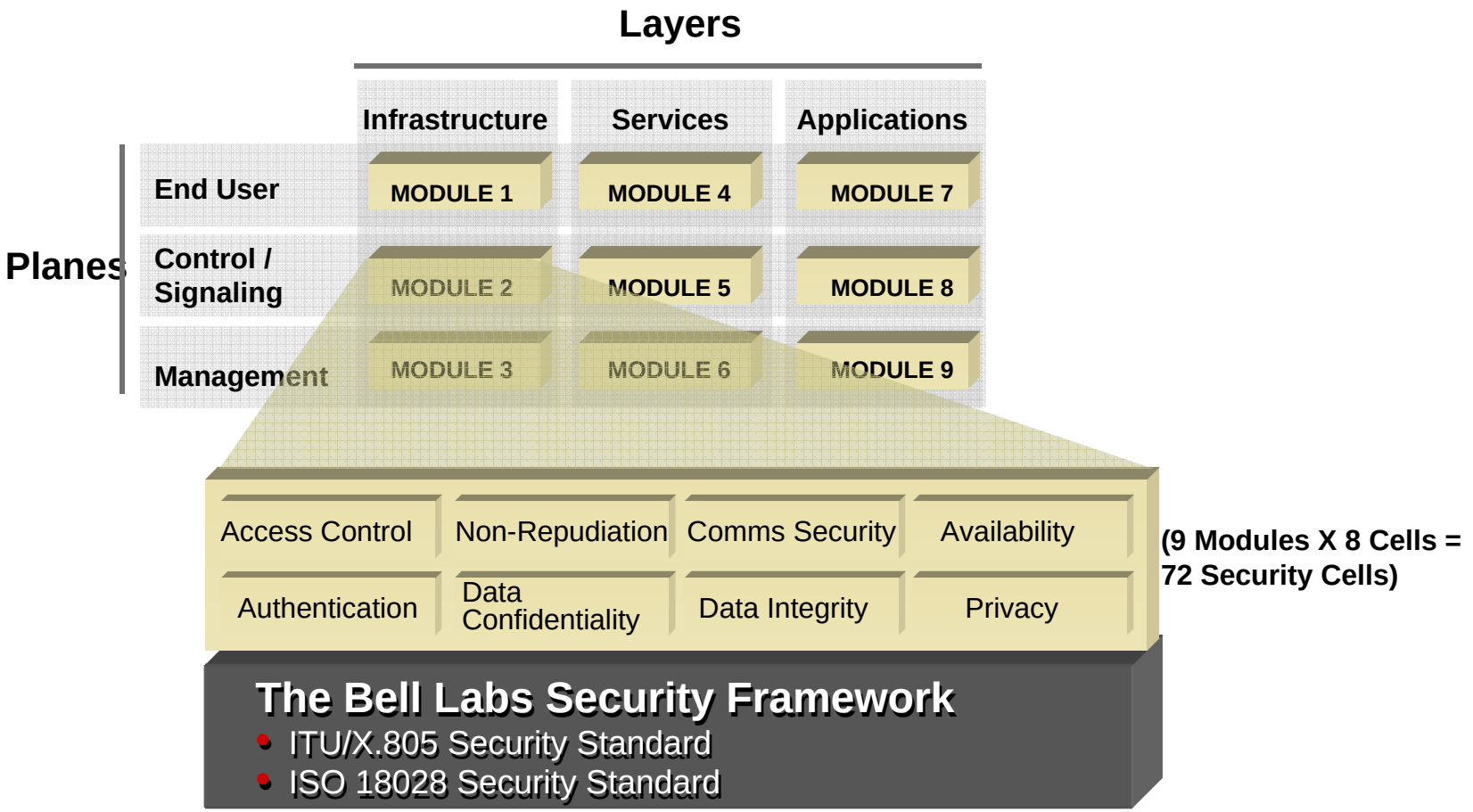
HOWEVER …There is a Downside

- With Integration comes Higher Probabilities of “Contamination”
- Interconnected to the high-threat environment of the Internet
  - DDOS – Malware – Hackers – Privacy Theft – Data Compromise
- IP addressable components potentially accessible from anywhere

A Key Contribution

The Bell Labs Security Framework

Building Security in the DNA of Complex Systems



(9 Modules X 8 Cells = 72 Security Cells)

ISO/IEC JTC1/SC27 N5179

ITU-T security building blocks

Security Architecture Framework
- X.800 – Security architecture
- X.802 – Lower layers security model
- X.803 – Upper layers security model
- X.810 – Security frameworks for open systems: Overview
- X.811 – Security frameworks for open systems: Authentication framework
- X.812 – Security frameworks for open systems: Access control framework
- X.813 – Security frameworks for open systems: Non-repudiation framework
- X.814 – Security frameworks for open systems: Confidentiality framework
- X.815 – Security frameworks for open systems: Integrity framework
- X.816 – Security frameworks for open systems: Security audit and alarms framework

Telecommunication Security
- X.805 – Security architecture for systems providing end-to-end communications
- X.1051 – Information security management system – Requirements for telecommunications (ISMS-T)
- X.1081 – A framework for specification of security and safety aspects of telebiometrics
- X.1121 – Framework of security technologies for mobile end-to-end communications
- X.1122 – Guideline for implementing secure mobile systems based on PKI

Protocols
- X.273 – Network layer security protocol
- X.274 – Transport layer security protocol

Security in Frame Relay
- X.272 – Data compression and privacy over frame relay networks

Security Techniques
- X.841 – Security information objects for access control
- X.842 – Guidelines for the use and management of trusted third party services
- X.843 – Specification of TTP services to support the application of digital signatures

Directory Services and Authentication
- X.500 – Overview of concepts, models and services
- X.501 – Models
- X.509 – Public-key and attribute certificate frameworks
- X.519 – Protocol specifications

Network Management Security
- M.3010 – Principles for a telecommunications management network
- M.3016 – TMN Security Overview
- M.3210.1 – TMN management services for IMT-2000 security management
- M.3320 – Management requirements framework for the TMN X-Interface
- M.3400 – TMN management functions

Systems Management
- X.733 – Alarm reporting function
- X.735 – Log control function
- X.736 – Security alarm reporting function
- X.740 – Security audit trail function
- X.741 – Objects and attributes for access control

Televisions and Cable Systems
- J.91 – Technical methods for ensuring privacy in long-distance international television transmission
- J.93 – Requirements for conditional access in the secondary distribution of digital television on cable television systems
- J.170 – IPCablecom security specification

Multimedia Communications
- H.233 – Confidentiality system for audiovisual services
- H.234 – Encryption key management and authentication system for audiovisual services
- H.235 – Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals
- H.323 Annex J – Packet-based multimedia communications systems – Security for H.323 Annex F (Security for simple endpoint types)
- H.350.2 – Directory services architecture for H.235
- H.530 – Symmetric security procedures for H.323 mobility in H.510

Facsimile
- T.30 Annex G – Procedures for secure Group 3 document facsimile transmission using the HKM and HFX system
- T.30 Annex H – Security in facsimile Group 3 based on the RSA algorithm
- T.36 – Security capabilities for use with Group 3 facsimile terminals
- T.503 – Document application profile for the interchange of Group 4 facsimile documents
- T.563 – Terminal characteristics for Group 4 facsimile apparatus

Message Handling Systems (MHS)
- X.400/ F.400 – Message handling system and service overview
- X.402 – Overall architecture
- X.411 – Message transfer system: Abstract service definition and procedures
- X.413 – Message store: Abstract service definition
- X.419 – Protocol specifications
- X.420 – Interpersonal messaging system
- X.435 – Electronic data interchange messaging system
- X.440 – Voice messaging system

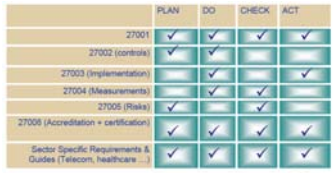
ITU-T Recommendations are available from the ITU website http://www.itu.int/publications/bookshop/how-to-buy.html (this site includes information on limited free access to ITU-T Recommendations)

Synergy Between ISO/IEC 27001:27005 and ITU-T X.805 / ISO,IEC 18028-2

The combination of ITU-T X.805 / ISO/IEC 18028-2 and ISO 27000 address business, and technical risks associated with information and network security

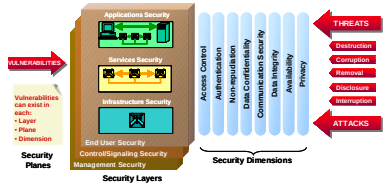
ISO/IEC 27001:27005

- **Provides standards for implementing, maintaining and improving an Information Security Management System to manage risk within the context of an organization's overall business environment.**



ITU-T X.805/ ISO,IEC 18028-2

- **Provides standards for detailed technical design, architecture, requirements, and test plans for the end-to-end network security solutions or individual products**

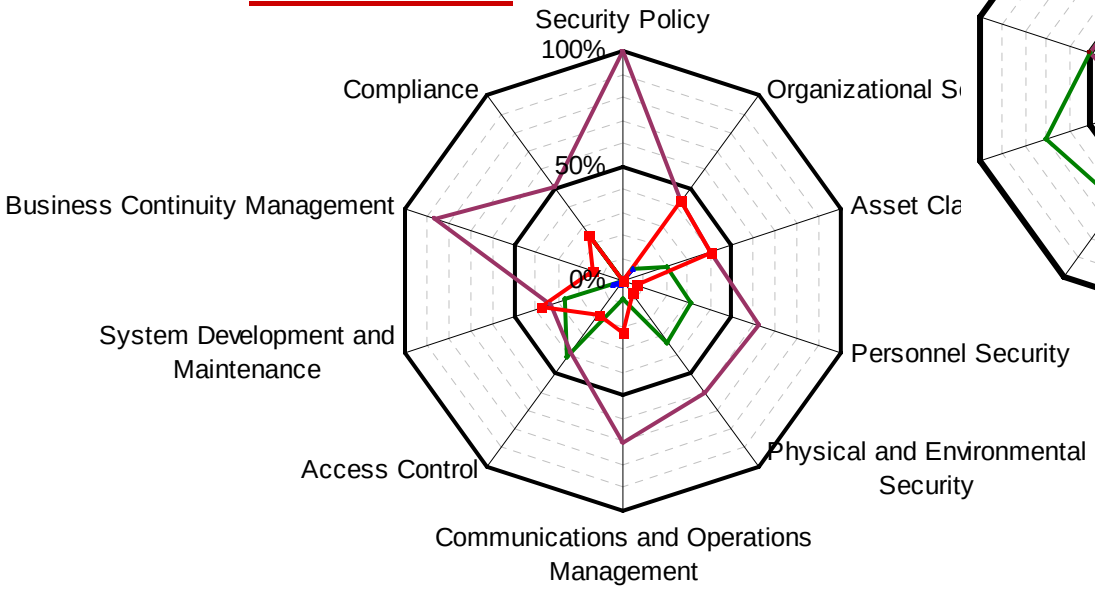


ISMS = Information Security Management Systems

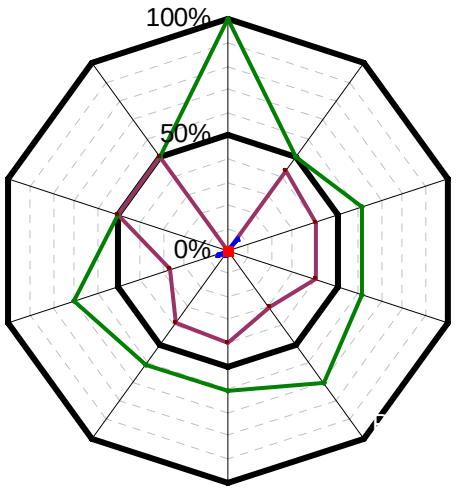
Example: Security Audits in Complex Systems

	Implemented	Partially/Planned to	Not Applicable	Not Implemented
Security Policy	0%	100%	0%	0%
Organizational Security	7%	43%	7%	43%
Asset Classification and Control	20%	40%	0%	40%
Personnel Security	31%	63%	0%	6%
Physical and Environmental Security	33%	60%	0%	7%
Communications and Operations Management	8%	70%	0%	23%
Access Control	41%	39%	2%	18%
System Development and Maintenance	26%	33%	4%	37%
Business Continuity Management	0%	86%	0%	14%
Compliance	25%	50%	0%	25%

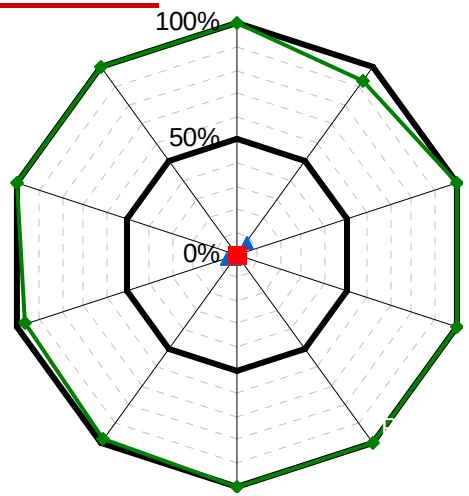
Current View



In Two Months



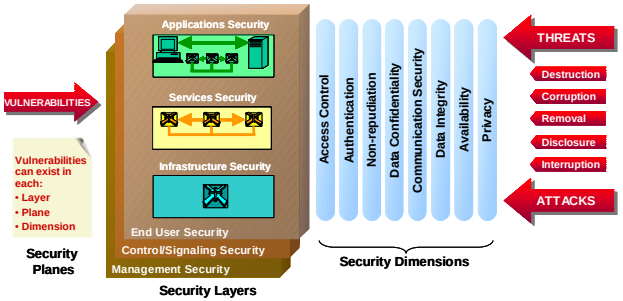
Ready for Audit



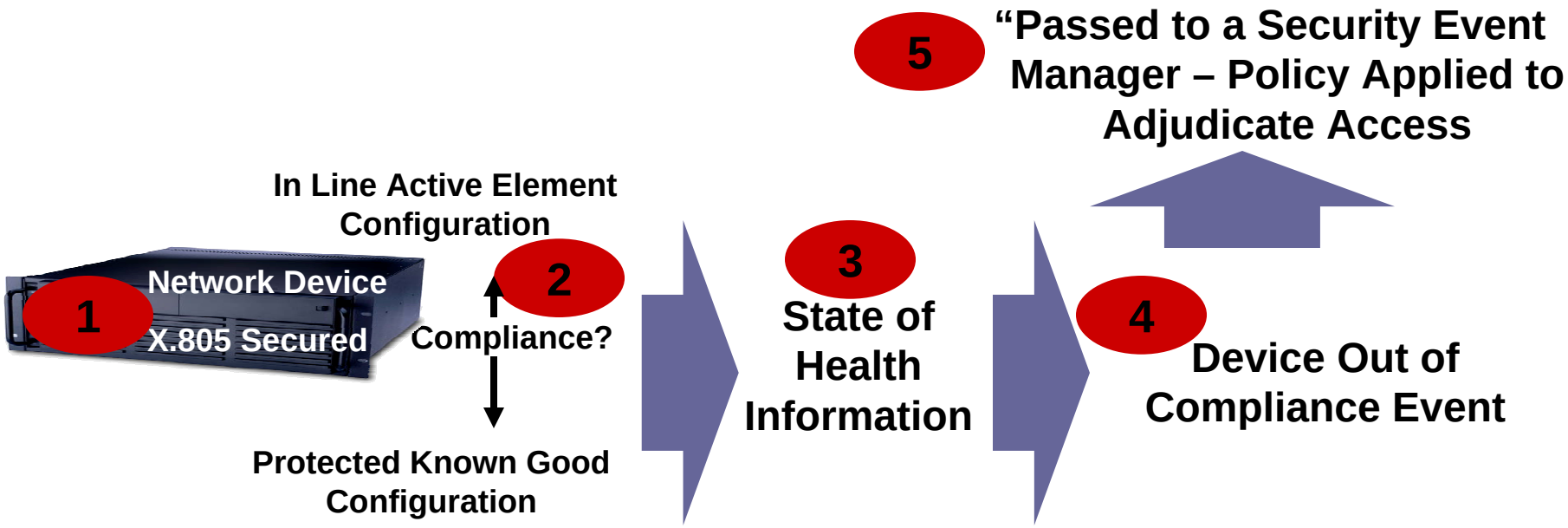
The Bell Labs Security Framework

It applies…

- Real Security Assessments – not a paper tiger
- Common Criteria – specification and standardization
- Security in the Product Development Process
- The foundation for building
  - secure products, that build
  - secure systems, that build
  - secure infrastructures
- A common security language for every level of granularity



Step One of the Process



The Bottom Line of Security

- IP based systems underpin the workings of each of the national infrastructures. And they are in a highly vulnerable state.
- The old approach to security will not reduce this vulnerability – no matter how much we spend and no matter how good we get at patching.
- Solutions must resolve in the time-space of the exploitation window. Reactive approaches cannot resolve within this time-frame.
- We need a new security paradigm – Trust Based Computing is a necessity – an urgent and critical necessity.
- The supply-demand dynamic is the only market force that will cause this change – if you demand it the market will supply the solutions.