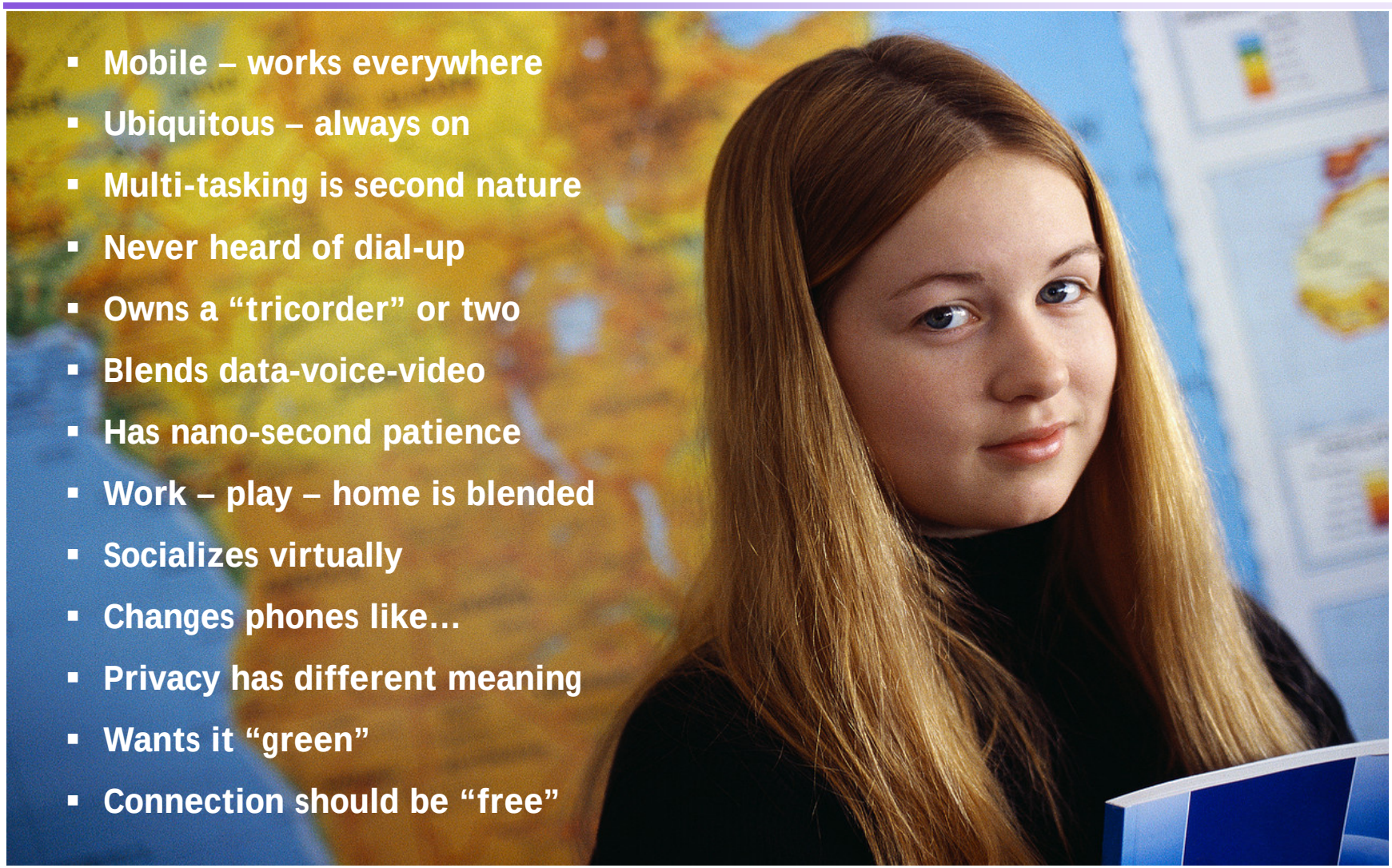
A Question of Security

Carlos Solari
Bell Laboratories

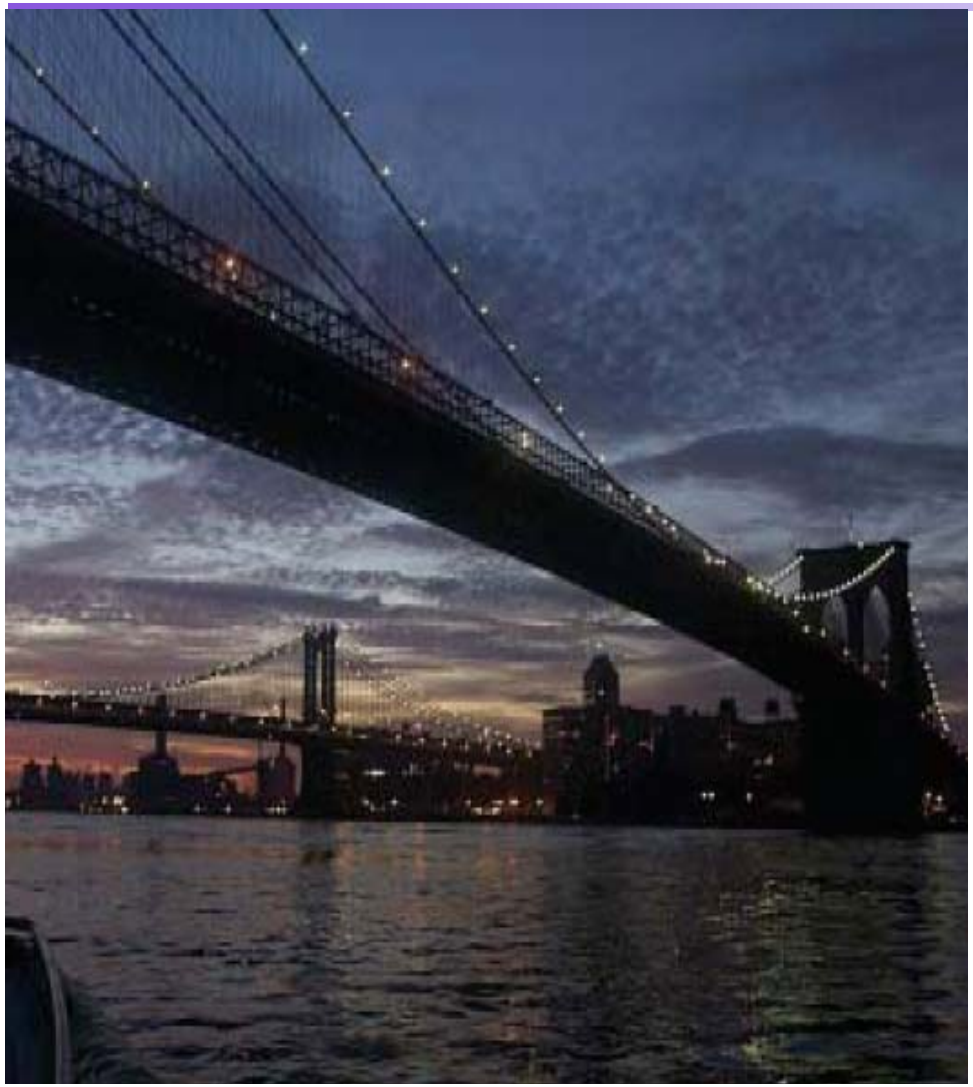
Alcatel·Lucent

Meet the New Consumer



- Mobile – works everywhere
- Ubiquitous – always on
- Multi-tasking is second nature
- Never heard of dial-up
- Owns a “tricorder” or two
- Blends data-voice-video
- Has nano-second patience
- Work – play – home is blended
- Socializes virtually
- Changes phones like…
- Privacy has different meaning
- Wants it “green”
- Connection should be “free”

A World Increasingly Dependent on IP-Based Systems



CRITICAL INFRASTRUCTURE SECTORS

- Agriculture
- Food
- Water
- Public Health
- Emergency Services
- Government
- Defense Industrial Base
- Information and Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemical Industry and Hazardous Materials
- Postal and Shipping

The Tensions of Change – Some Interesting Parallels

Business Enablers

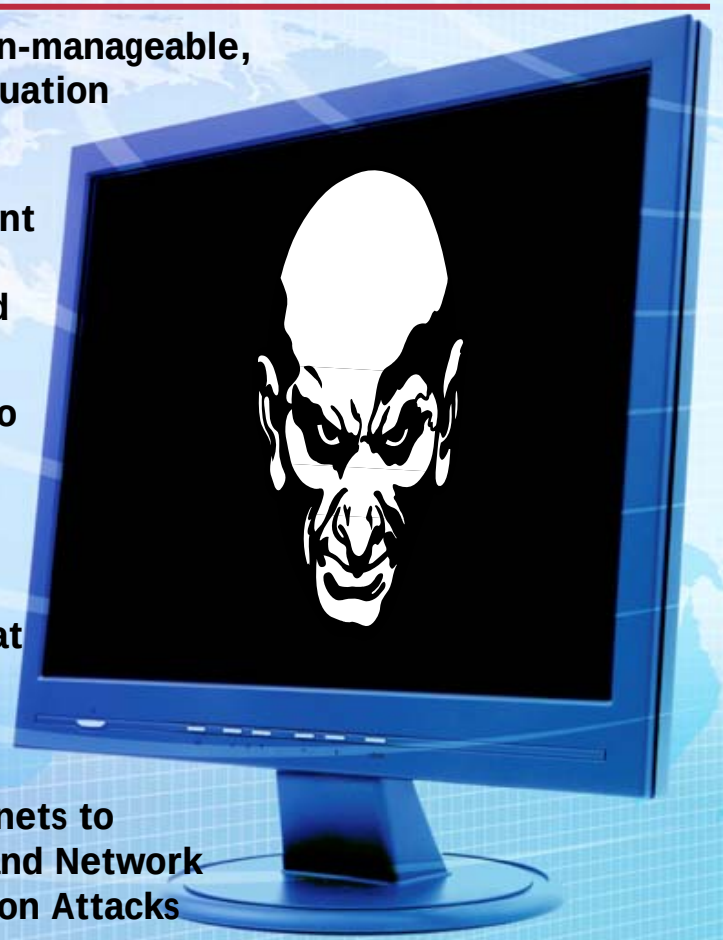
- Blogs
- VoIP
- Wireless
- PDAs
- Social Networking
- Different Roles
- Location Based Services
- Text Messaging
- Web 2.0 services
- New applications

Challenges

- Stovepipe Architecture
- Stovepipe Technicians
- Don't Get Hacked
- Blending of Physical-Personnel-Logical Security
- Outsourcing
- Crisis: DR/BC
- Compliance Audits
- The Speed of a Crisis
- What is private?
- Records Management
- Different Departments
- …with diff requirements

The Challenge Gets Tougher – Not Easier

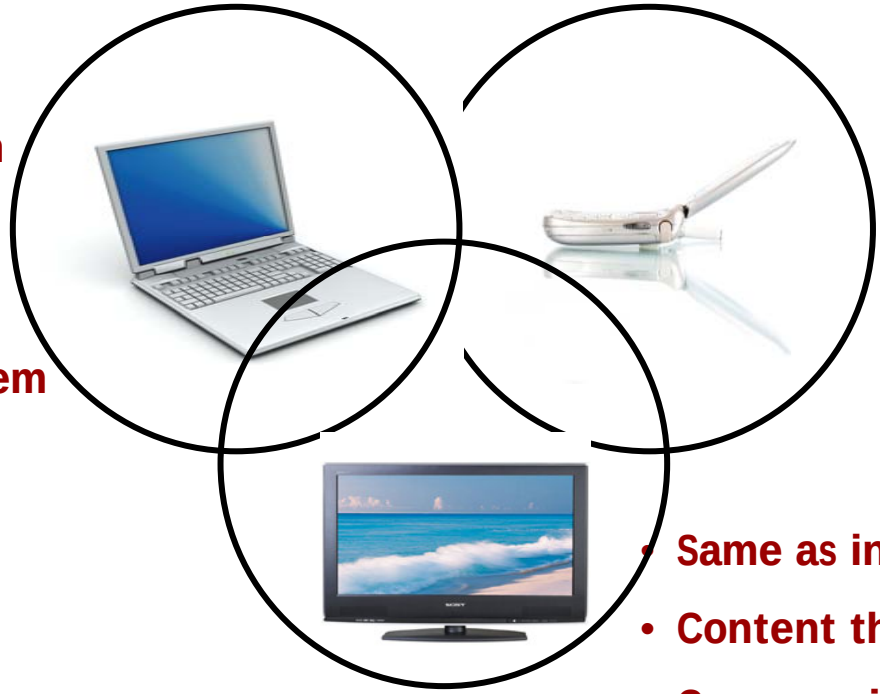
- **Blacklists defenses ineffective** — Reactive and ineffective for zero-day attacks
- **Increased network complexity** — Complexity increases vulnerability
- **Exploit Window Smaller** — Threats exploit impact business faster than we detect-respond
- **Data Leakage** — More personal data online – sold or leaked
- **Data Flooding** — SPAM-SPIT-SPASMS tough to separate wanted info
- **Point Solutions** — Security un-manageable, missing situation awareness
- **Weak Links Prevalent** — Inconsistent security, un-trusted
- **Lack of Universal Standard** — Difficult to integrate security
- **Data Control & Integrity** — Security controls at the data level
- **Sophisticated Cyber Crime** — From botnets to rootkits and Network Penetration Attacks



Complexity? Aint Seen Nothing Yet

- Convergence: all things IP means benefits, but also risk…
- Threats transfer between data, voice and video…
- With international reach – beyond the law

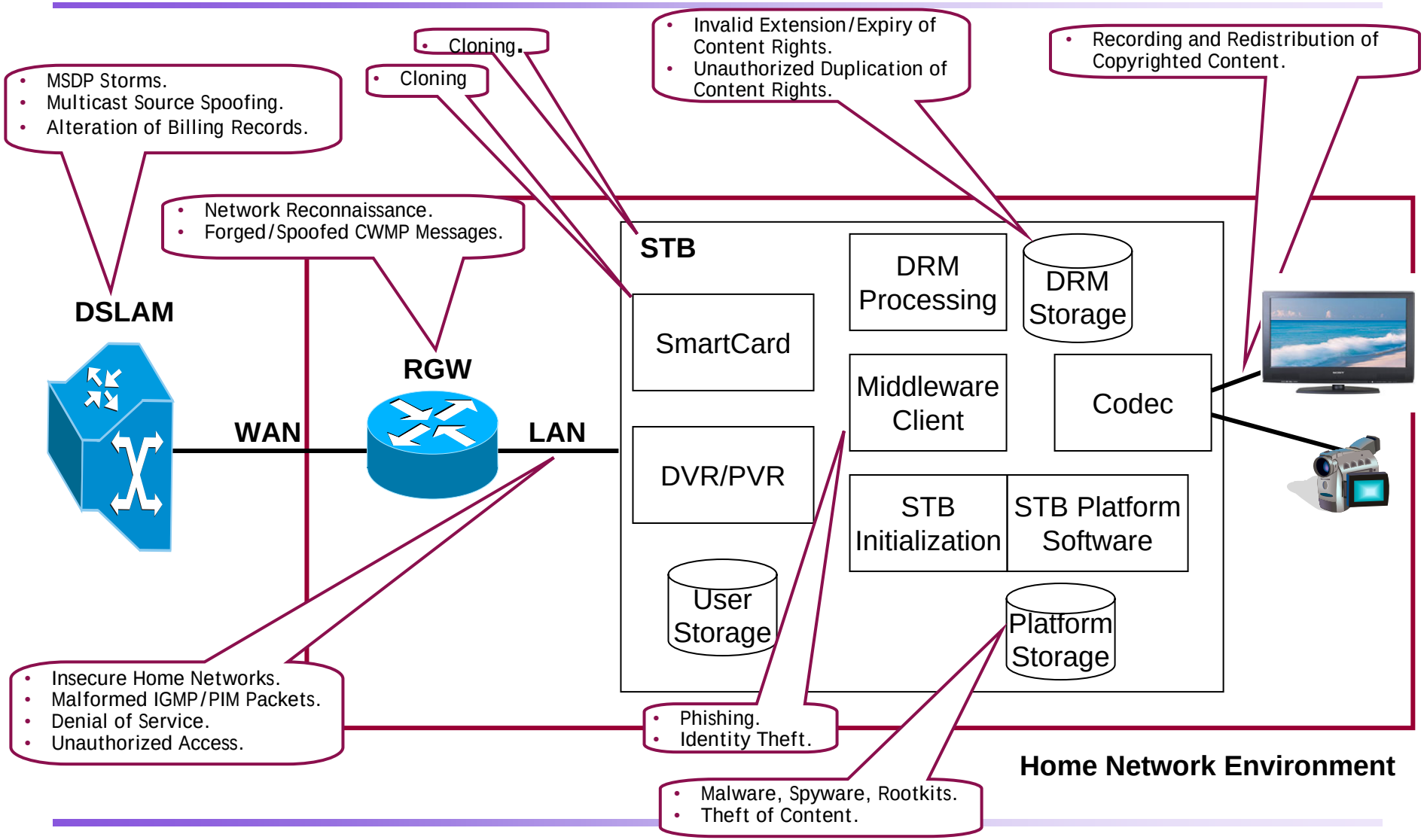
- **Deperimiterization**
- **Data theft**
- **Scams**
- **Compromised system integrity**



- **Same as in data +**
- **Consume RF b/w**
- **Battery drain**
- **Identity theft**
- **"SPIT"**

- **Same as in data +**
- **Content theft**
- **Compromised privacy**

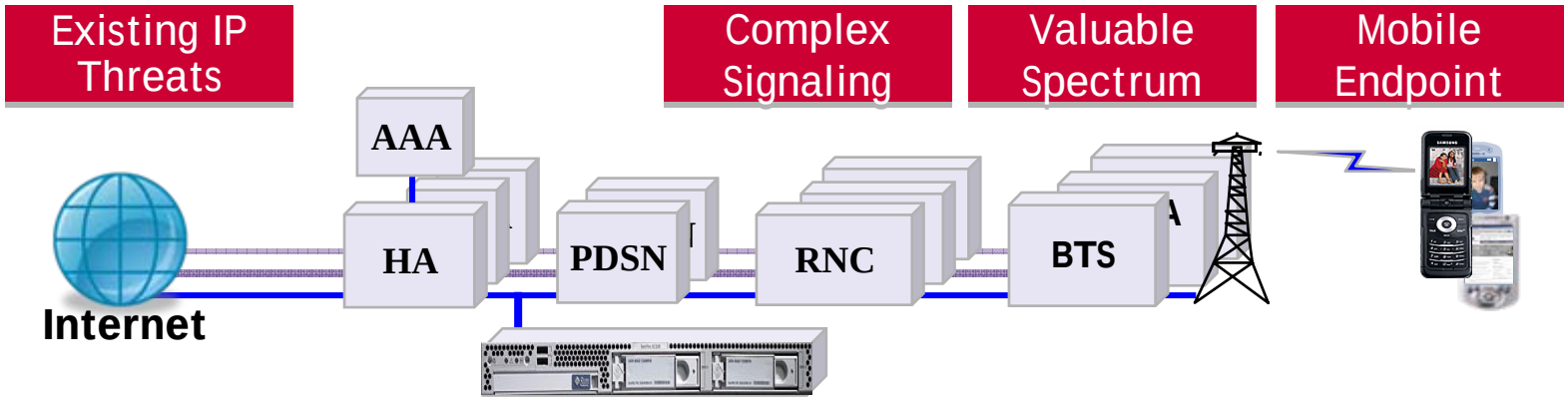
The Next Generation TV (IPTV) is a Good Example – not your Father's TV



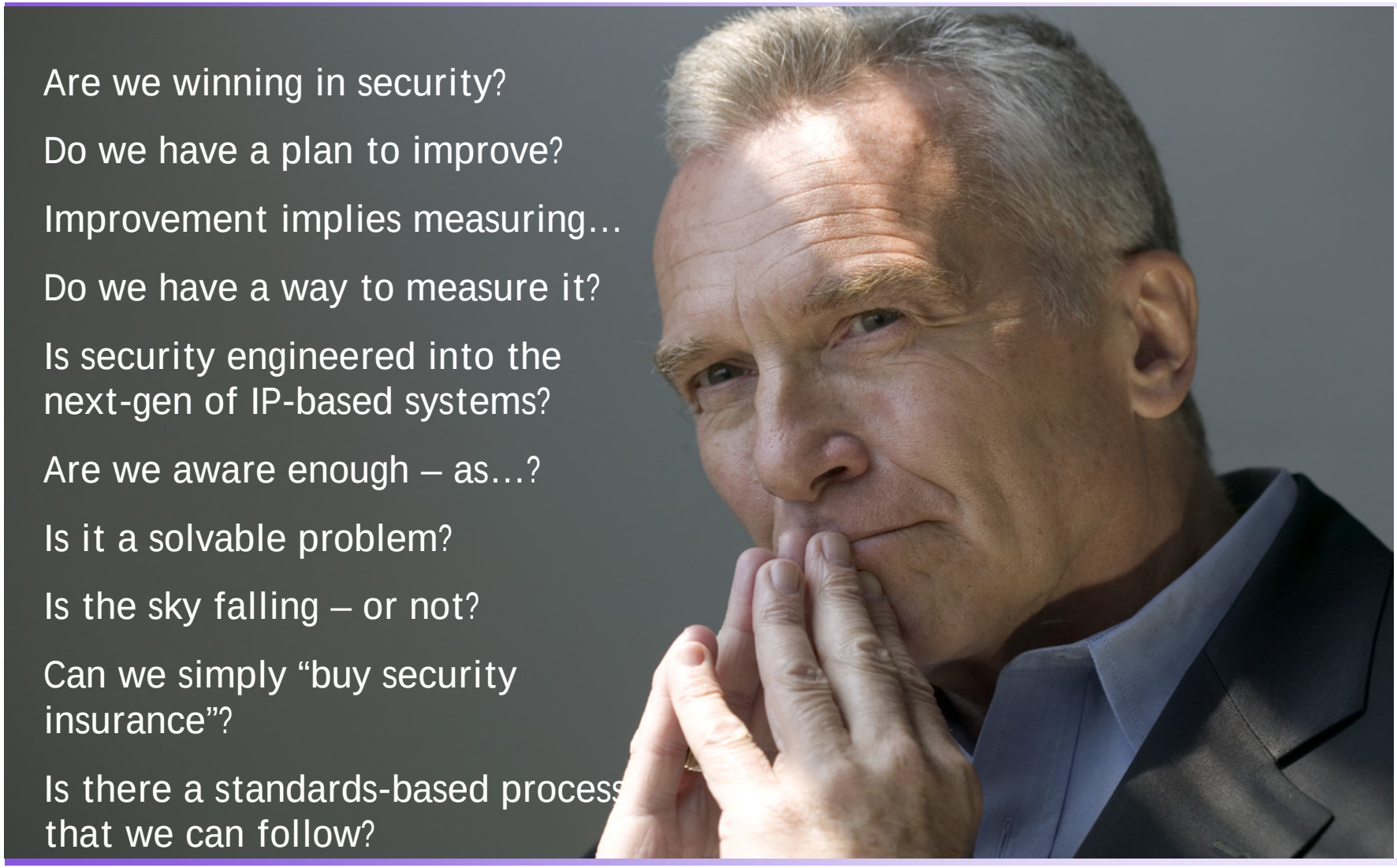
Another Good Example: Wireless Broadband Security

Wireless broadband (3G and 4G) network security (CDMA EVDO example)

- Inherently much more vulnerable (ex: b/w capacity in RF versus DSL)
- Detection and Response must occur in real-time…or it is too late
- Little experience with this threat – yet everything is going IP wireless



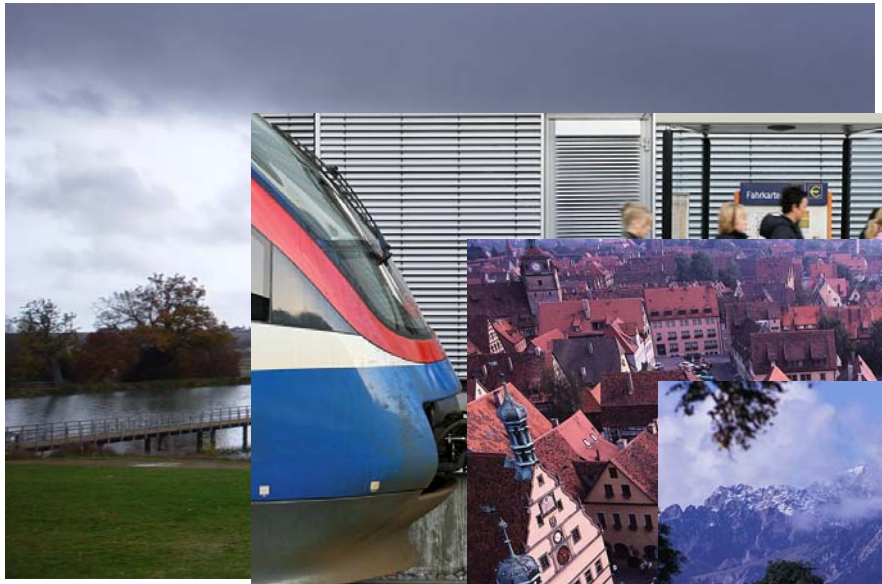
Some Important Questions We Should Be Asking…



- Are we winning in security?
- Do we have a plan to improve?
- Improvement implies measuring…
- Do we have a way to measure it?
- Is security engineered into the next-gen of IP-based systems?
- Are we aware enough – as…?
- Is it a solvable problem?
- Is the sky falling – or not?
- Can we simply “buy security insurance”?
- Is there a standards-based process that we can follow?

Re-Architecting Security

Beginning with Our Customer…



A global workforce – not feudal. The perimeter is where we work, live and play

Mobile, ubiquitous access

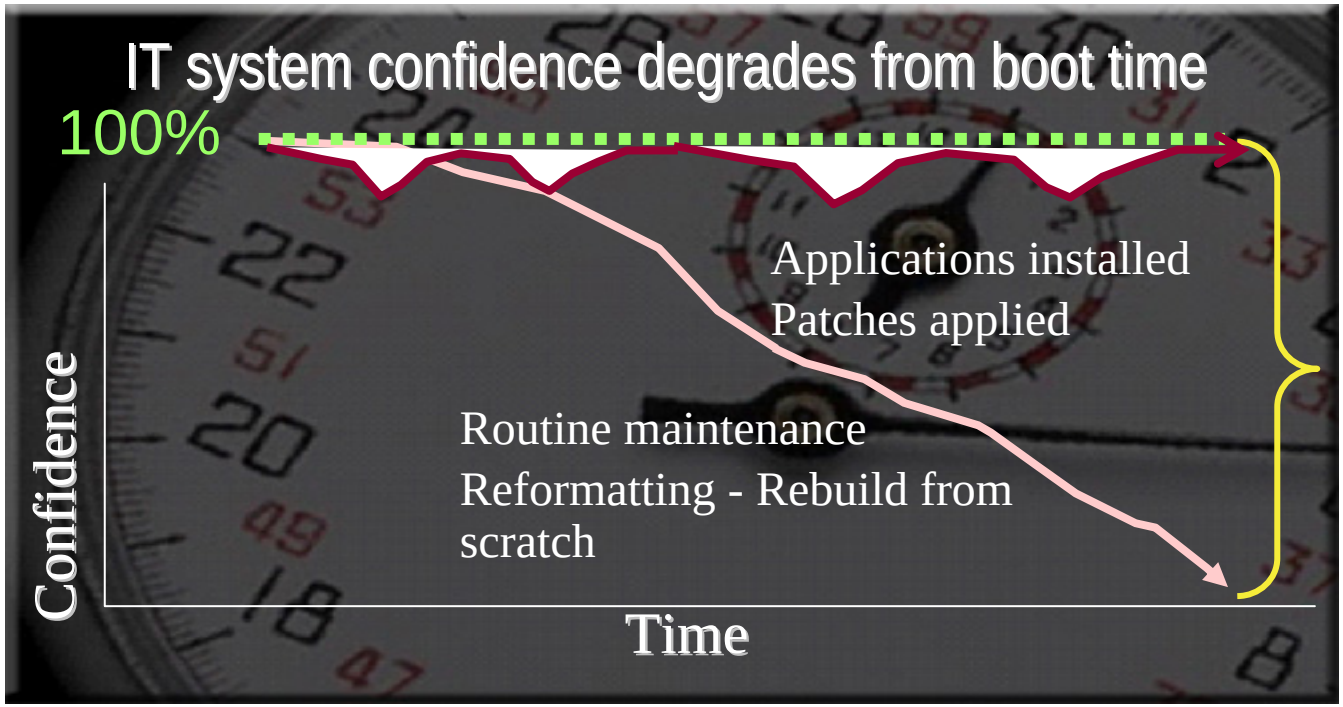
Global yes, but local and family friendly

In harmony with our culture, our environment

To Improve Security - We Must Measure It

The ability to establish and maintain an awareness of the state-of-integrity of a system component

- White-list basis of security operations
- To apply a policy respondent to the state-of-integrity

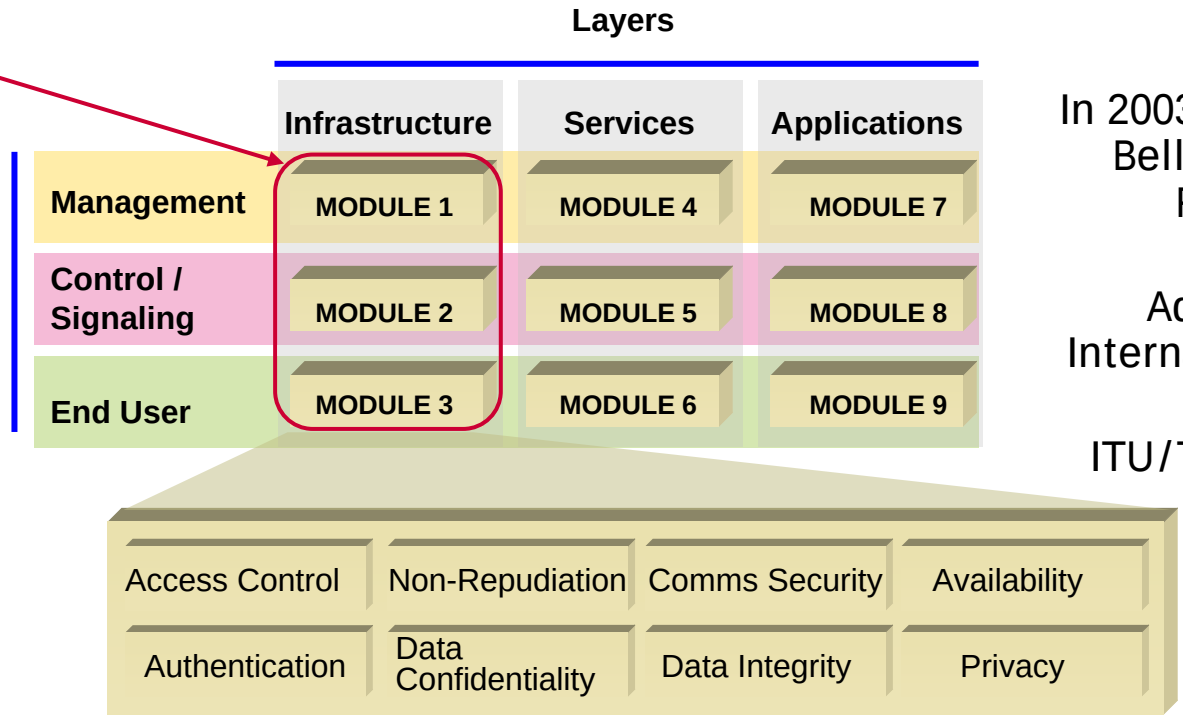


"State-of-integrity" measured, reported, enforced by policy

The unknown… when will it fail, what is the cause, what was lost?

(by permission from SignaCert)

To Improve Security - We Must Design It In



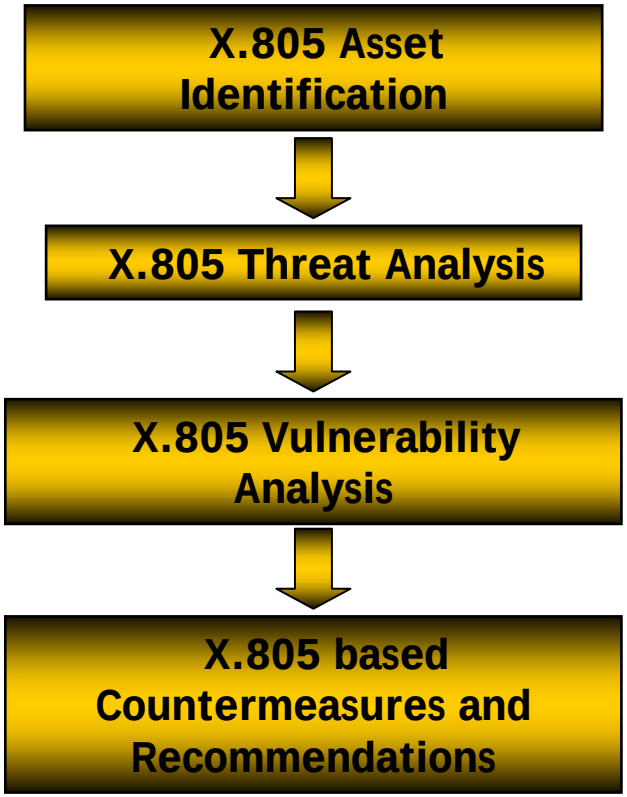
In 2002 – looked for a framework…could not find one…

In 2003…Developed the Bell Labs Security Framework

Adopted as an International Standard

ITU/T x.805 and ISO 18028

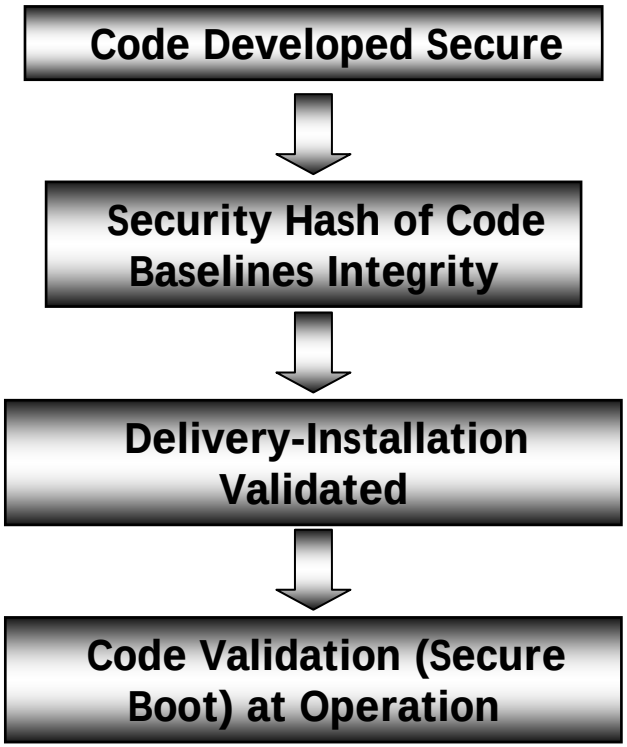
To Improve Security – Work a Consistent Process



Benefits

- Stop Re-Inventing the Wheel
- Shared Security Procedures
- Completeness
- Rigorous Process
- Supports Certification
- Creates Transparency
- Scales: Element to System level
- Repeatable
- Exchange of Security Information (APIs) to speed detection-response

To Improve Security – A Positive Security Model



- Lifecycle Control: Creation thru Operation
- Eliminate Ambiguity
- Allows Validation
- The “micro-level’ config control
- Supports new US Gov requirements
- A positive trust-model
- Verifiable trust – not faith based
- Needed for expanded transaction based Internet
- Scales to highly sensitive networks
- Such as satellite control/signaling

My Top Five Lessons: (1) CIO - CISO Partnership is Critical

- The partnership has to be tight
- Exercise different roles
- The CIO must be the balancer…
- The CISO - authorized to act
- Offer choices beyond “No”…after all the point of security is about taking “acceptable” risks

My Top Five Lessons: (2) A Security Framework is a Must

- Too much complexity to simply ad lib
- Allows you to baseline (where are you)
- Map your path to where you want to be
- Manage the expectations
- Builds your business case
- Binds the investment to a business goal
- Otherwise you are operating in fire brigade mode – guaranteed to lose

My Top Five Lessons: (3) Establish & Maintain Positive Control

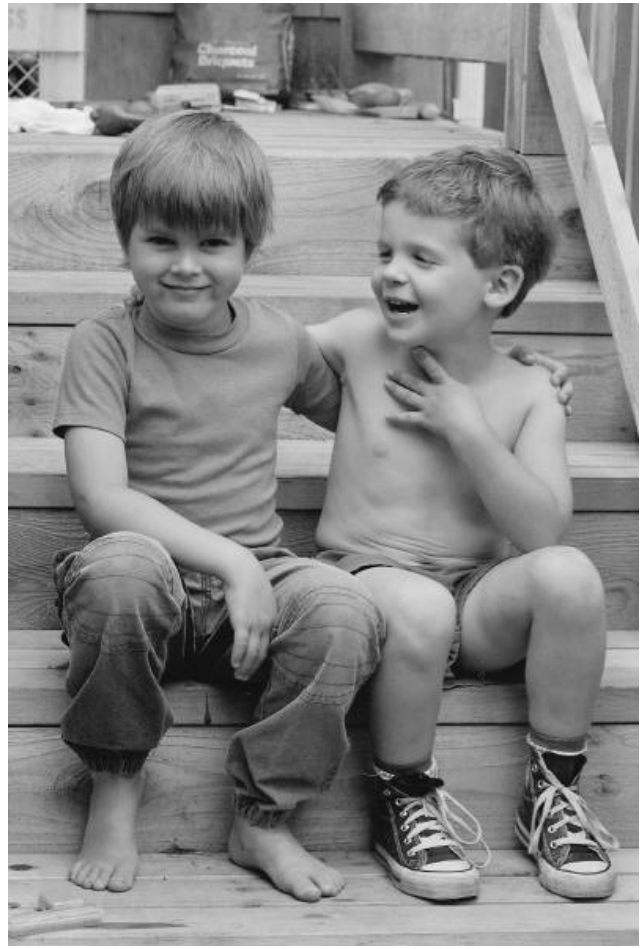
- From Macro (programmatic), to Mid (Network Access), to Micro (Integrity Attestation)
- What are the assets – in real-time
- What is the authorized configuration
- What are the acceptable Levels of Risk
- System integrity validated
- Data integrity validated
- Detect - Respond faster than the threat can have its impact

My Top Five Lessons: (4) Plan for the Crisis

- Three stages of planning: (1) Will happen tomorrow…(2) in 90 days… (3) next year…
- You get graded on 2 things. The crisis will make you hero or goat
- You should test your plan - really
- Good assumption: the crisis will happen
- How will you communicate during the crisis – when communications is down?
- All crisis situations can be managed with the ability to communicate – converse is also true – the crisis cannot be managed without communications

My Top Five Lessons: (5) Make Friends

- You will need them – no joy in going solo
- With industry, peers, business owners…
- Business partners
- The market does not have all the answers
- You need the researchers on your team
- Working the tough problems
- Academia – Bell Labs ☺



A Few Words of Wisdom…from the School of Hard Knocks

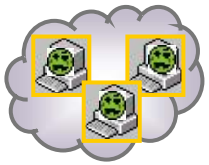
- From your computer-savvy 3 year old:
  "I TCP/IP – but mostly IP"
- Most important kindergarten indicator of your future success:
  "Plays well with others"
- Statements you don't want to be making in hindsight:
  - I didn't expect they would hit us
  - We did not have time to test the crisis plan
  - It was a unique attack – no one could have planned for this
  - We were still getting ready
  - They did not give me the budget that would have prevented this security breach

Not Theory – Real Threats with Consequences

A Worm Attack

- The story – an infected laptop
- Consequences

Social Networking Access



- The story – download contacts
- Consequences

A Cyber-Criminal Attack – What If…

- The story: Your databases are encrypted by the CC
- They give you a choice – pay or lose the business
- Consequences: Public exposure, extortion, loss of brand confidence…only bad choices