

Mobile Computing: Security On The Move Securing Wireless Internet

GTC East - The New York Digital Government Summit



Simon Mizikovsky

September 23, 2009

10,000 feet view of this talk

Multiple dimensions to mobile security

- Networks have evolved

1G → 2G → 3G → 4G

- Applications have evolved

Cellular Voice → Email, VPN → Multimedia Download → Mobile Internet

- Users have evolved

Convenient to have a cell phone (early 90's). Can I afford it?

MUST have a 'mobile device' to see what's happening

Mobile Multimedia P2P Upload & Download to stay in touch and be relevant!

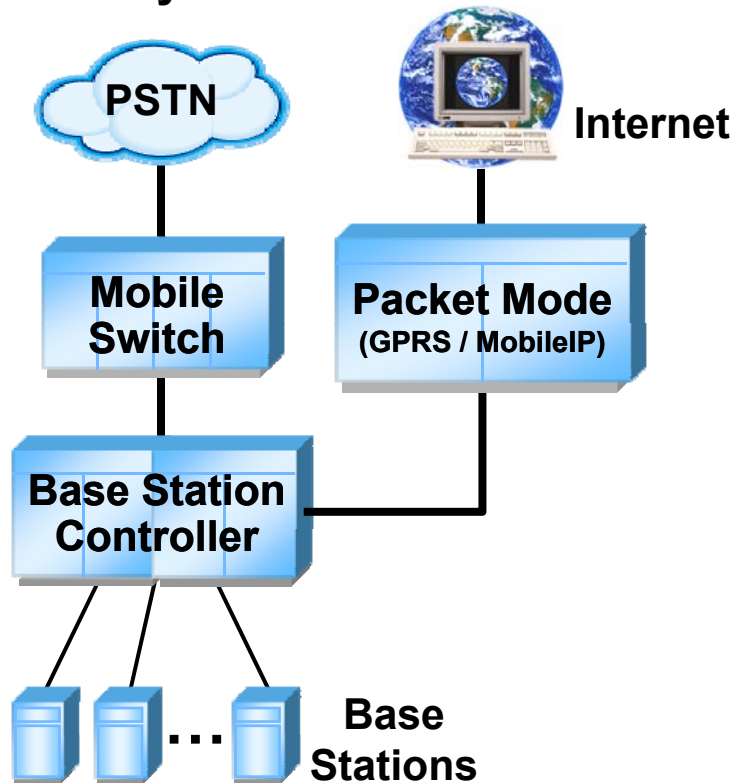
Securing the enigma of mobile broadband?

- Secure each dimension based on needs and capabilities

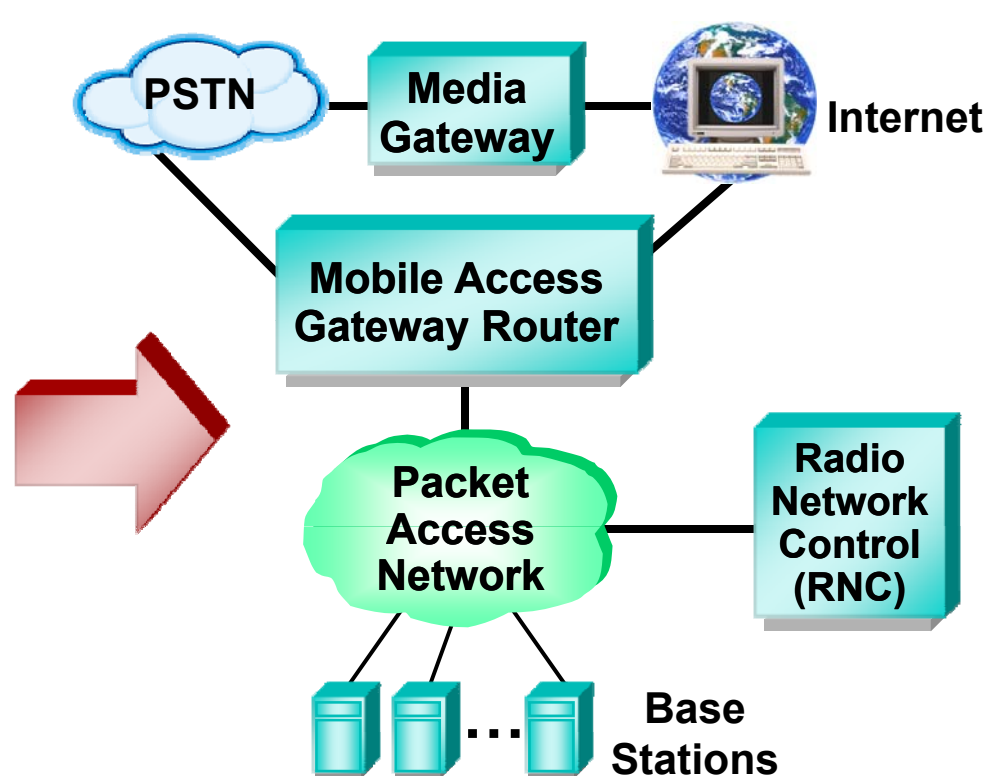
Discussion on changing needs of mobile security and pointers to solutions. Not a Tutorial!!

Wireless Network Architecture: 2G to 3G

Today's Wireless Networks



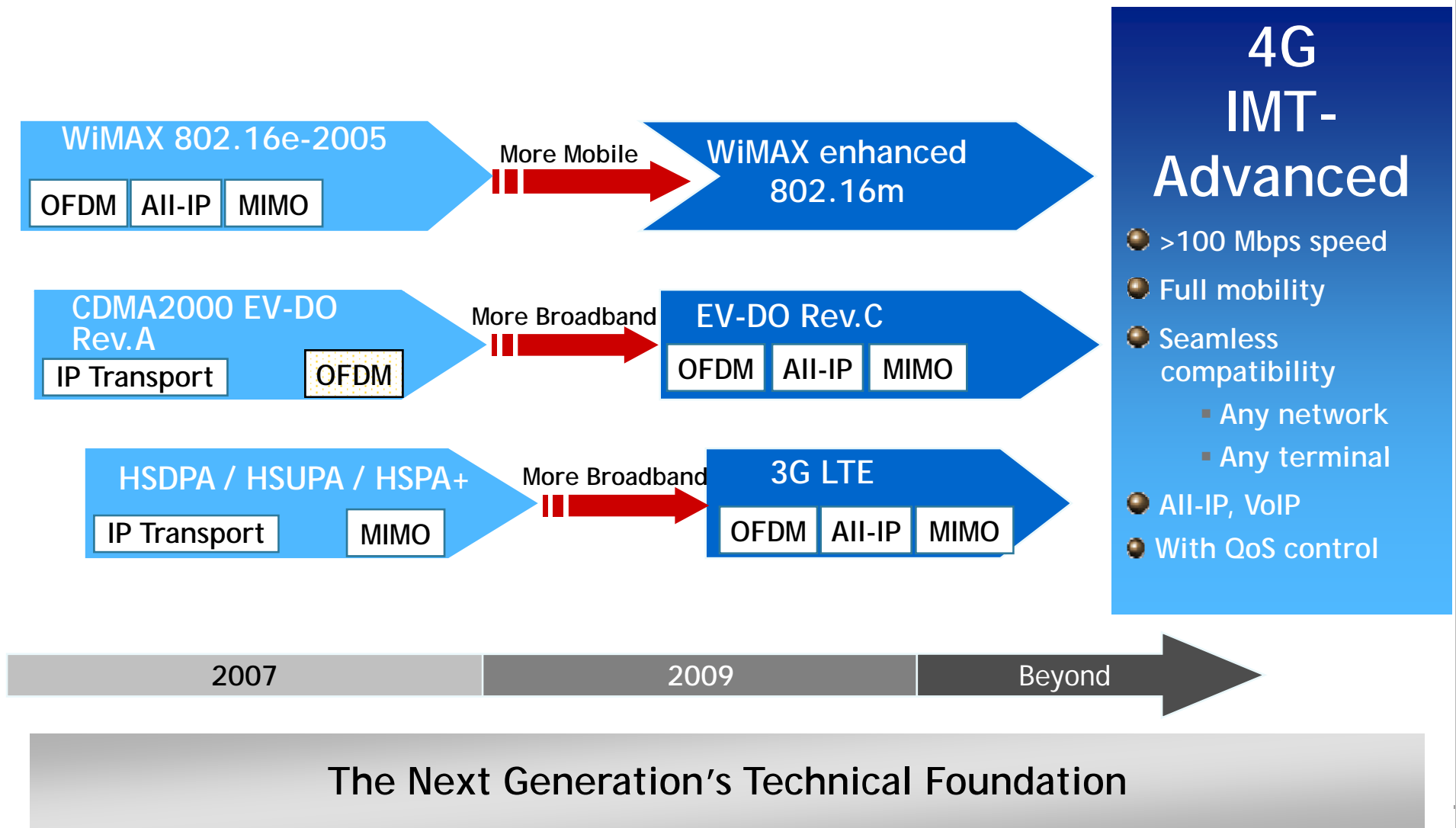
Third Generation Networks



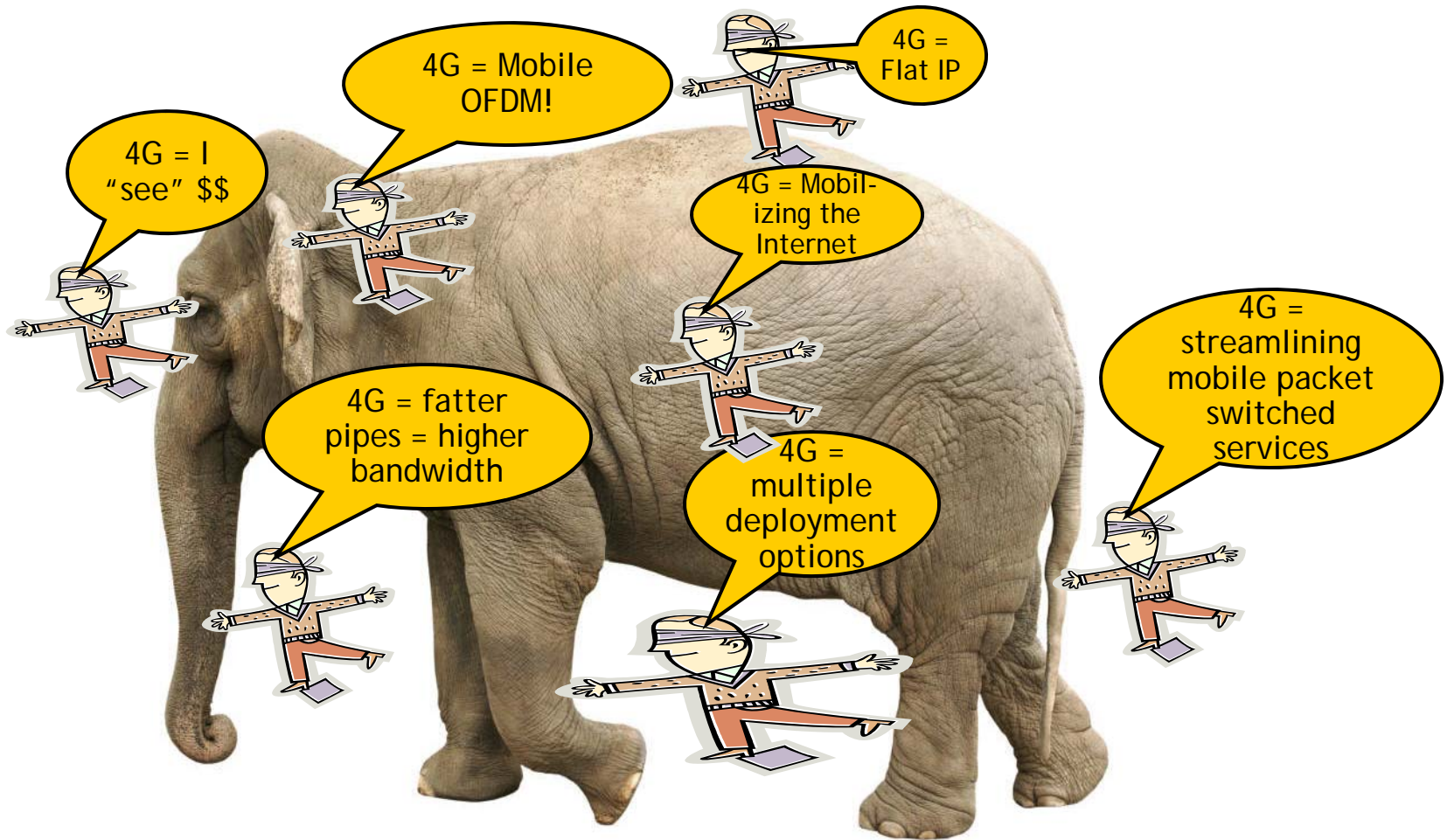
Capability Implications (2G ⇒ 3G)

- **Air Interface:** Increased voice capacity & data rates (9.6 kbps ⇒ Mbps)
- **Transport/Switching:** Circuit switched ⇒ Packet routed
- **Interconnect:** Voice to PSTN, Data to Internet ⇒ Voice & Data to Internet

Charting the Course to 4G



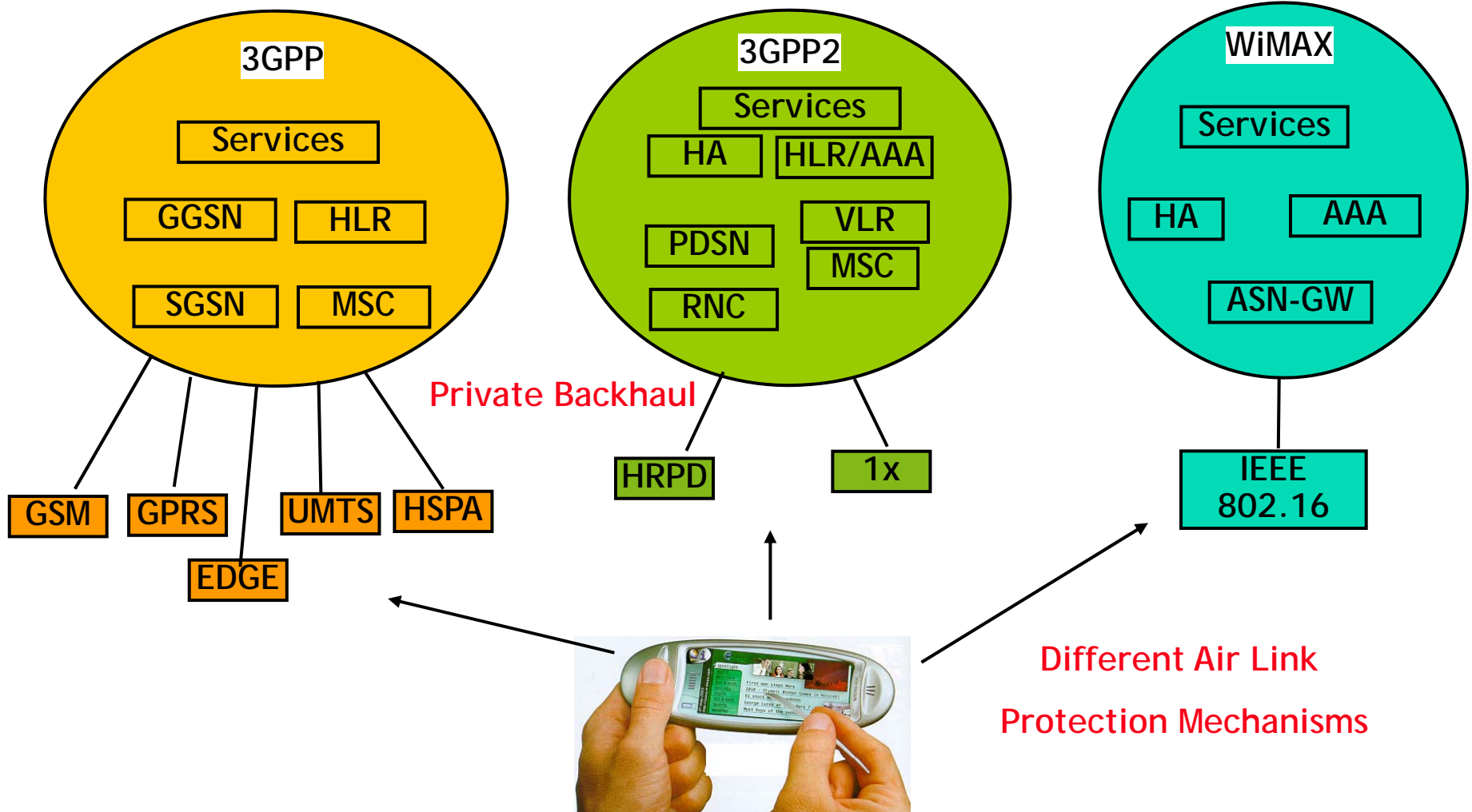
What is 4G?



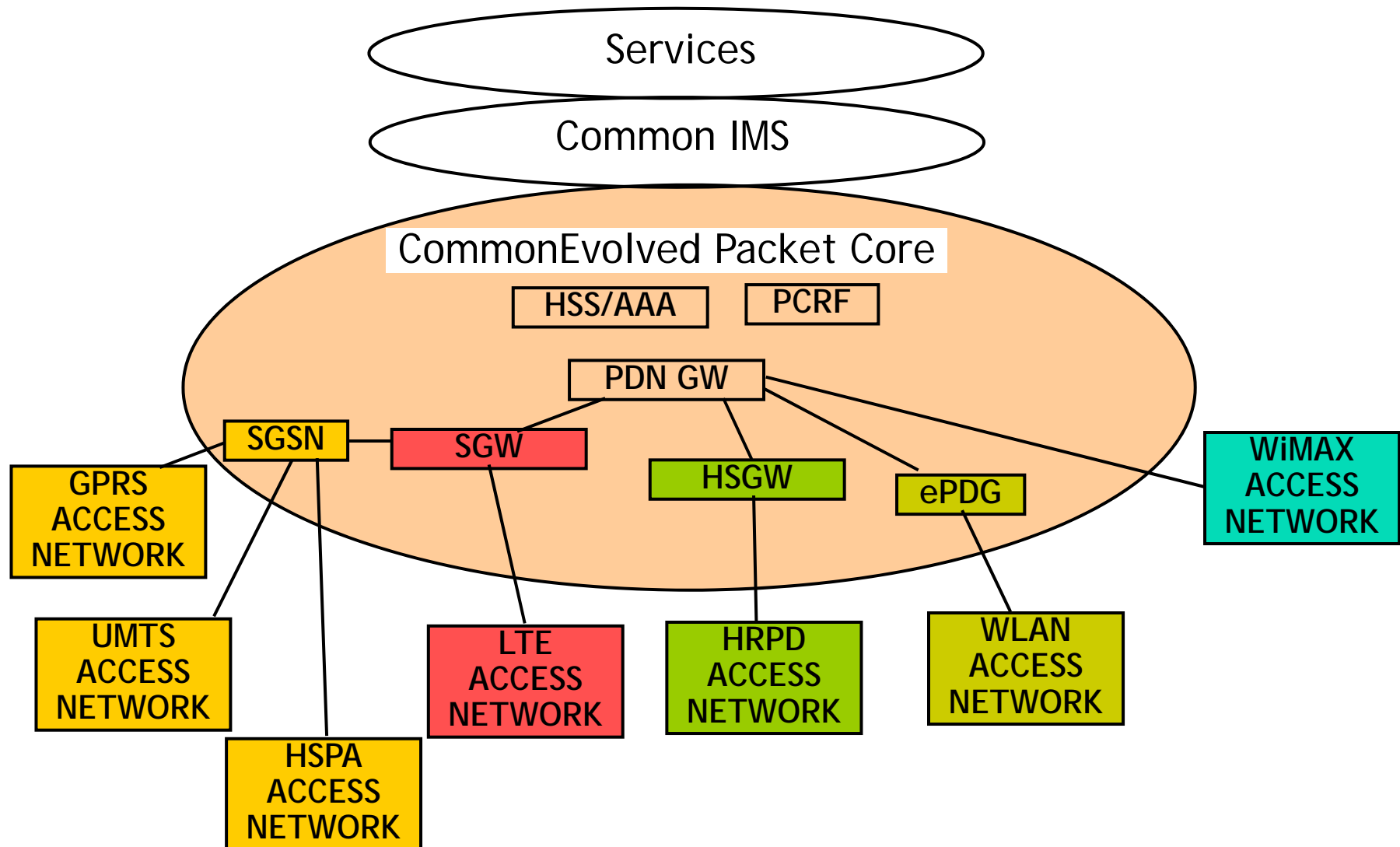
Next Generation = The entire elephant. Security across multiple layers.

Current Situation - Multiple Core Networks

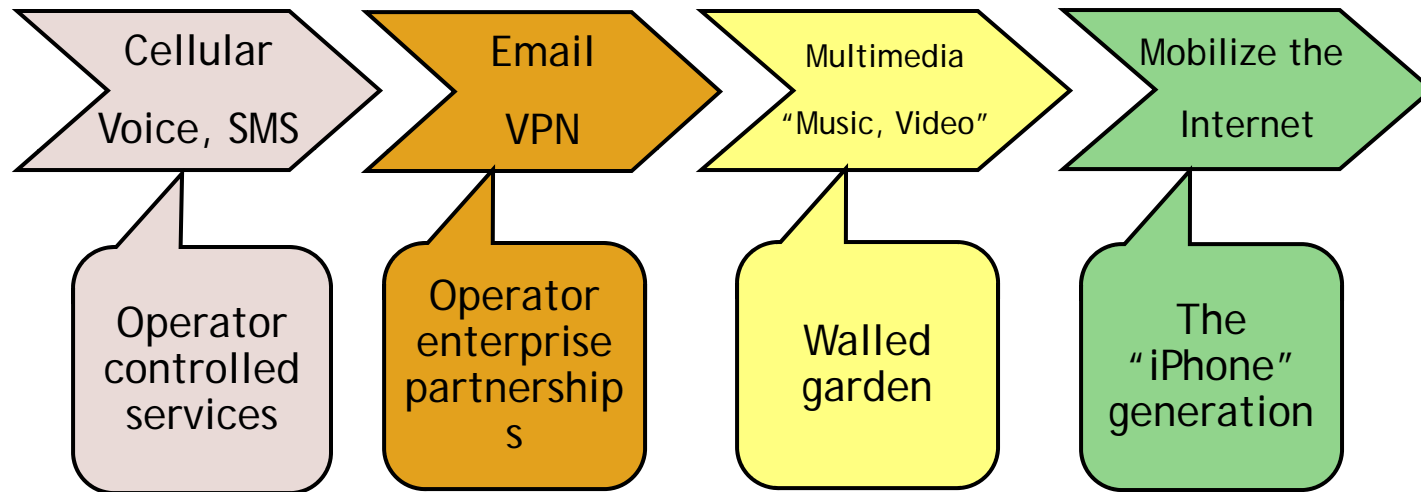
Different Core Vulnerabilities



Evolution of Networks: Common Evolved Packet Core



Evolution of Applications



Mobile Applications: Securing this "colorful" evolution; Who is responsible for what?

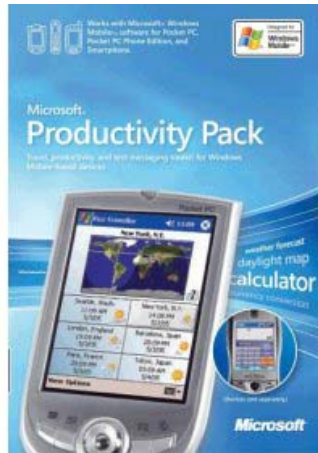
Evolution of mobile subscriber



Convenient!
Hmm. Pay for it?



Morning
Infotainment



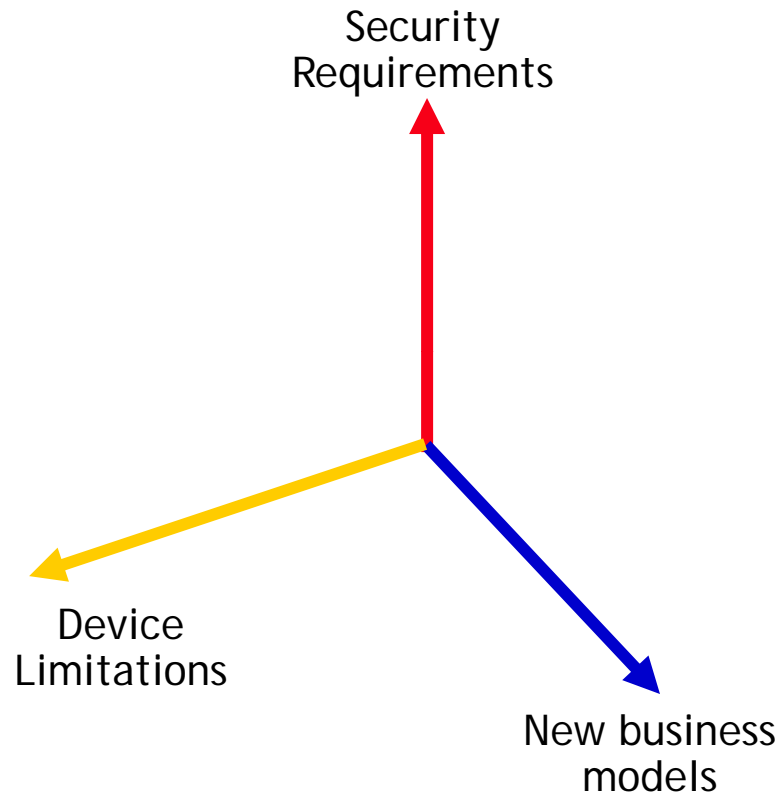
Productivity
During the day



Got to send
the news out!

Mobile subscriber needs increasing, but is security improving?

Next generation security conundrum



Changing landscape: Multiple orthogonal dimensions

Multiple security requirements

- Authentication, User Privacy
- Securing service layer
- Securing the network
- Securing Applications
- Securing Devices

Devices are challenged

- Battery capacity, computing power
- Cost, form-factor

Business models are changing

- Deployment models
- Ownership of bandwidth, application

Early goals of mobile security

Prevent Unauthorized Access to System Resources and Services.

- Solution: Cryptographic Authentication of Users and Access Terminals.

Protect the Communication Session from tampering, eavesdropping, hijacking.

- Solution: Session Encryption and Integrity Protection

Select High Efficiency Methods applicable for Small Mobile Processors.

- Solution: Utilize symmetric cryptography, efficient protocols with error recovery, fast algorithms.

In addition: Privacy of User Identity

- Solution: Concealing Identity of the real user and communications equipment by Radio Channel Encryption or Scrambling.

Securing access; prevent fraud and by the way some privacy

3G Security Enhancements

ESA: Enhanced Subscriber Authentication

- Mutual Authentication of Mobile and Network to each-other
- Authentication of Message Contents Integrity
- Strong Authentication Protocols with Larger Keys (128-bit).

ESP: Enhanced Subscriber Privacy

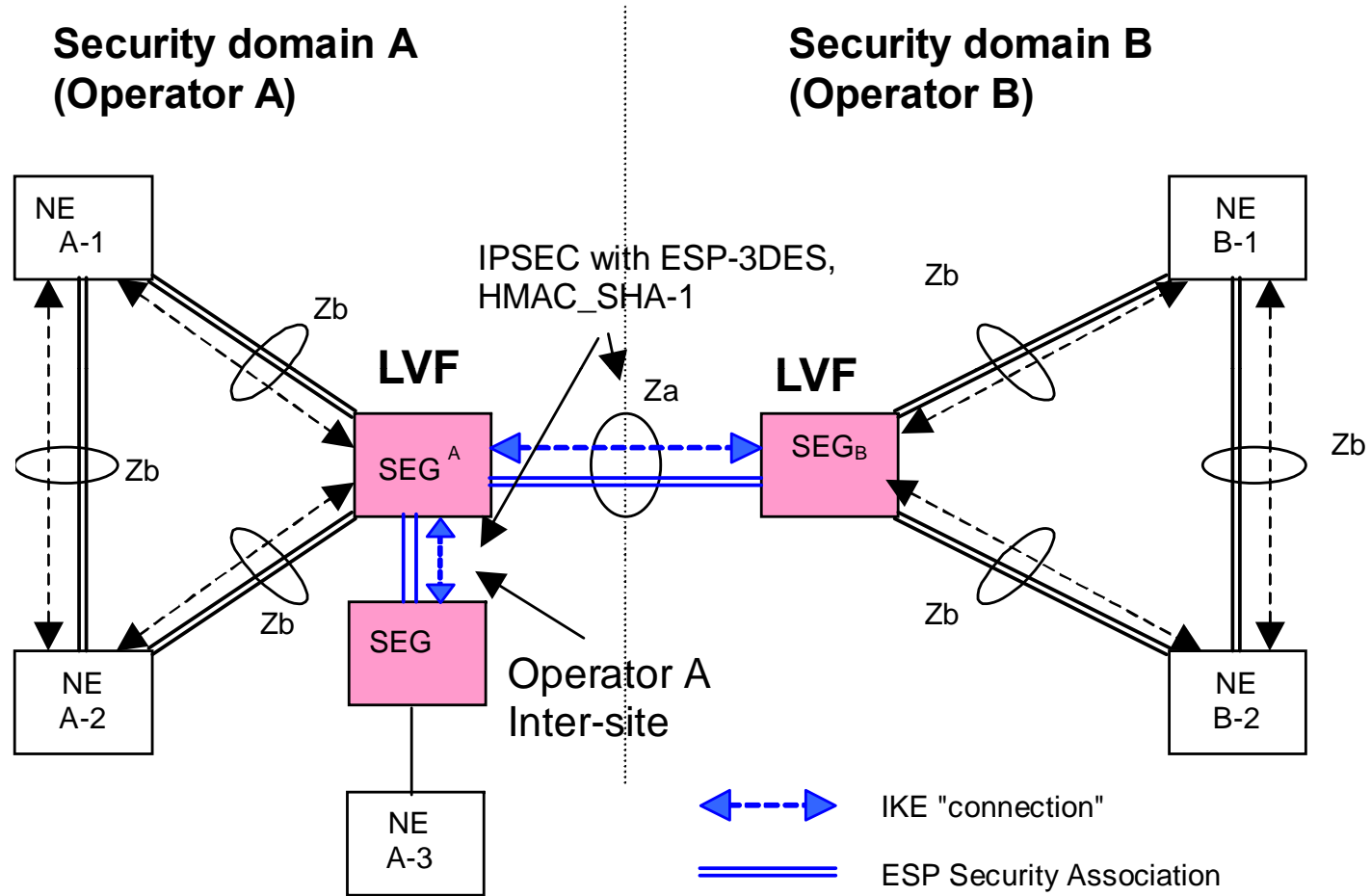
- Encryption of All Information Channels.
- Strong Encryption Algorithms with Larger Keys (128-bit).

Improvements in security

- Introduction of “proofs” of security, strong public algorithms.
AKA, Shazam, AES, SNOW, Hard bits and authentication functions, etc..
- Separation of link layer security from network layer security

Same goals as 2G, but significant improvements to protocols and algorithms

Network Domain Security: Backhaul and Core Transport



Only a subset of IKEv2 and IPsec specs is utilized. Pre-shared keys are expected.

IMS Security Architecture: Securing Service Control Plane

IMS is an IP-based Signaling Plane subsystem that allows running Multi-Media service by providing end-point Address Discovery and setting Communication Parameters.

Main IMS Security Attributes:

- Mutual Authentication of End Point IMS Client and HSS using IMS-AKA for IMS Admission Control.
- The “first hop” signaling between End Point Client (EP) and Proxy CSCF (P-CSCF) is secured by IPsec.

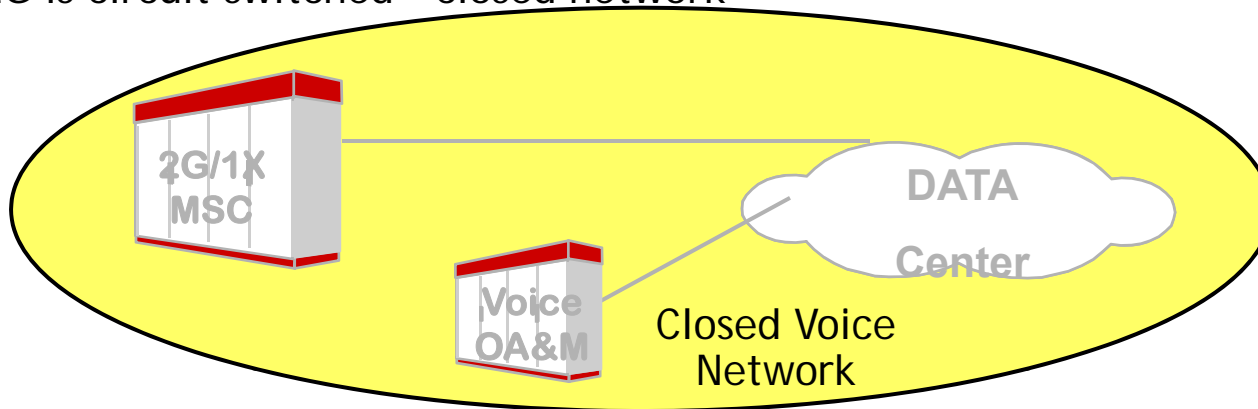
IMS signaling is transported “on the top” of Network Layer, and relies on Network Domain security.

IMS signaling can be used to transport the Key Management protocol for setting up the End-to-End Security for Multi-Media Clients at the End Points.

End-point (EP) authentication security

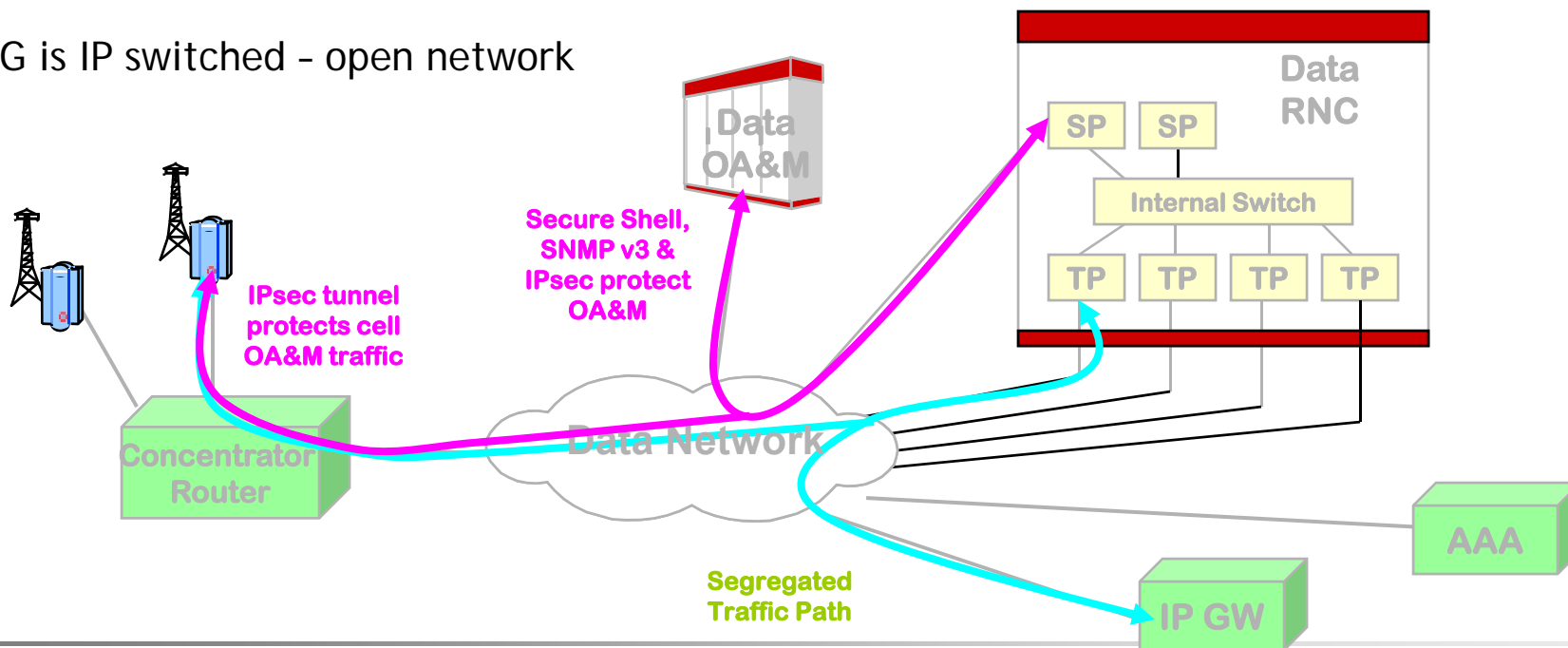
Securing the Management Plane

2G is circuit switched - closed network



Evolving from a "closed" voice network to an open data network- Management plane security outside the scope of standards

3G is IP switched - open network



What is Flat IP and Why is Security even More Important?

- **What is Flat IP, and Why?**

- Consolidation of wireless functions at the edge
 - All Access Network is collapsed in a single IP-aware Base Station
- Evolution from existing systems
 - Capacity improvements (cross-layer optimization)
 - Reduced complexity, ease of management and upgrades

- **What about security? Securing the cell-site!**

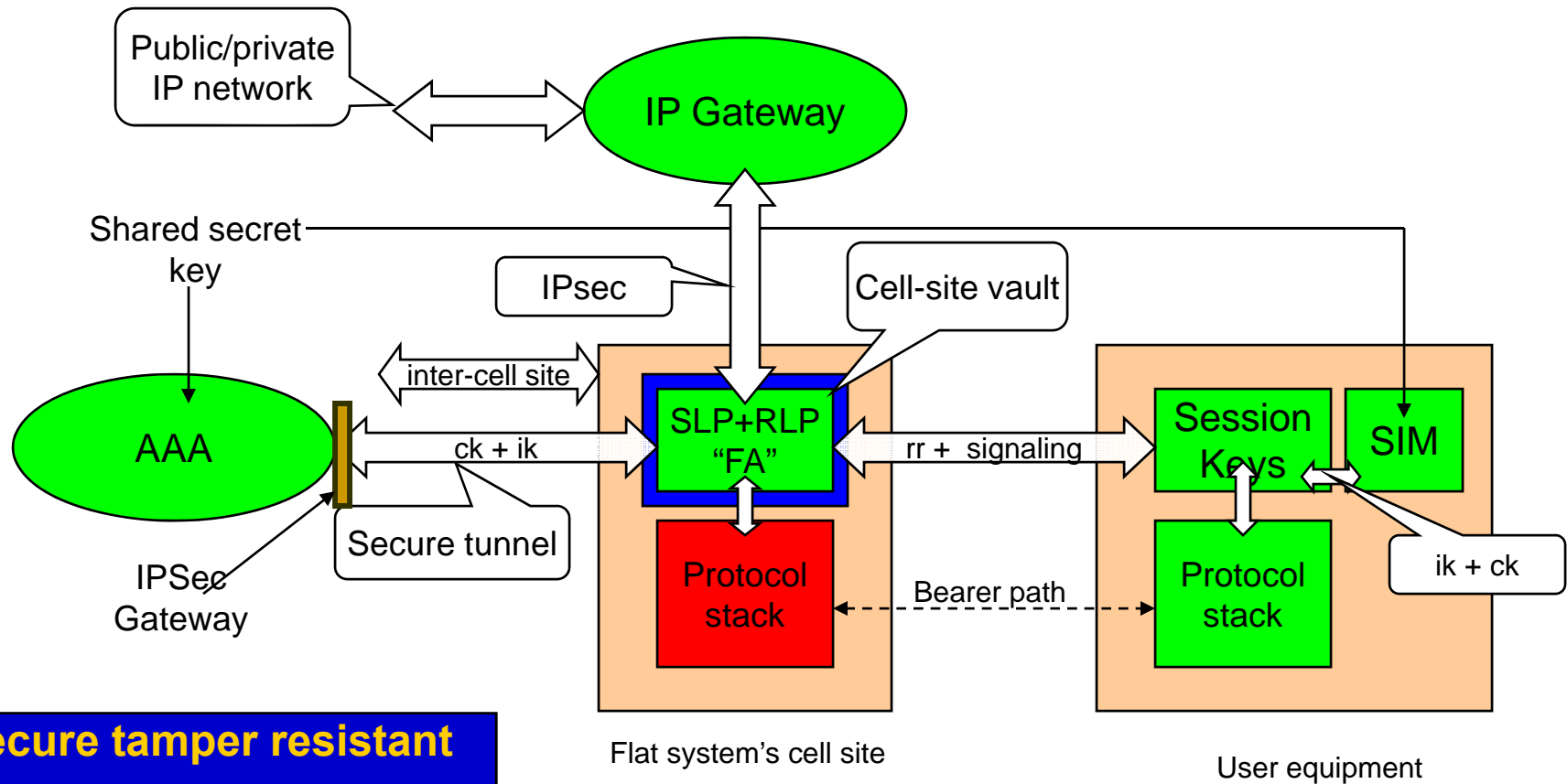
- Cryptographic security, not physical security
 - Tamper resistant, secure computing environment
 - Secure interfaces
- Protection against intrusion, eavesdropping, DoS, etc

Flat IP: Security not an after-thought

Flat IP security architecture

Cell-site vault provides:

1. Physical security for all session keys maintained by cell site
2. Performs ciphering and integrity protection for user and signaling plane
3. Secure tunnels to home agent and AuC/AAA



**Secure tamper resistant
computing environment**

Other 4G+ considerations - Beyond Flat IP

Multiple deployment options - Security architecture “evolving”

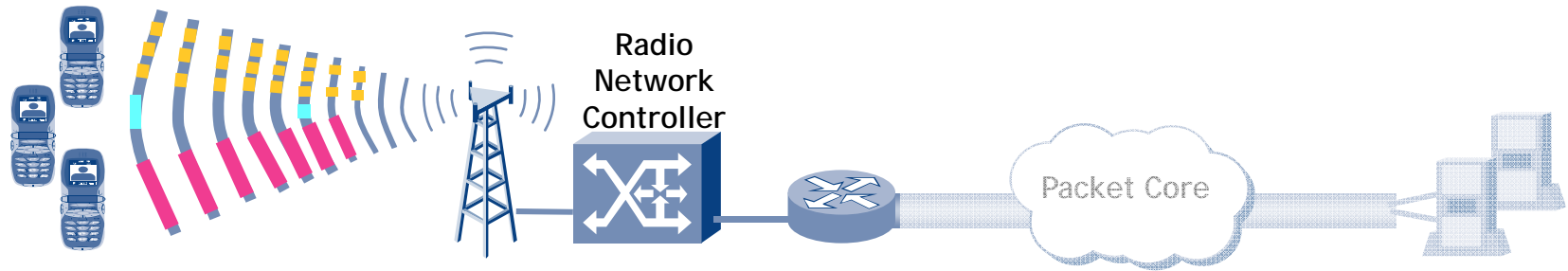
- Macro cellular - high mobility environments
- Micro cellular - hot spots and coverage holes (low mobility)
- Pico cellular - enterprise environments with licensed spectrum
- Femto cellular - home environments with licensed spectrum

Network layer security: From CMIP to Simple IP with PMIP

- Security assumptions
 - Mobility Agent is in secure environment: Node specific keys
 - Mobility Agent is in insecure environment: User specific keys
- Key bootstrapping problems
 - Multiple solutions being defined in standards based on network assisted “single-sign-on”

New network protocols and deployment options require fresh look

IP services over Wireless: New Paradigms to Attack!



- VPN Users can Consume on Average, 10x the Airtime as Typical Users

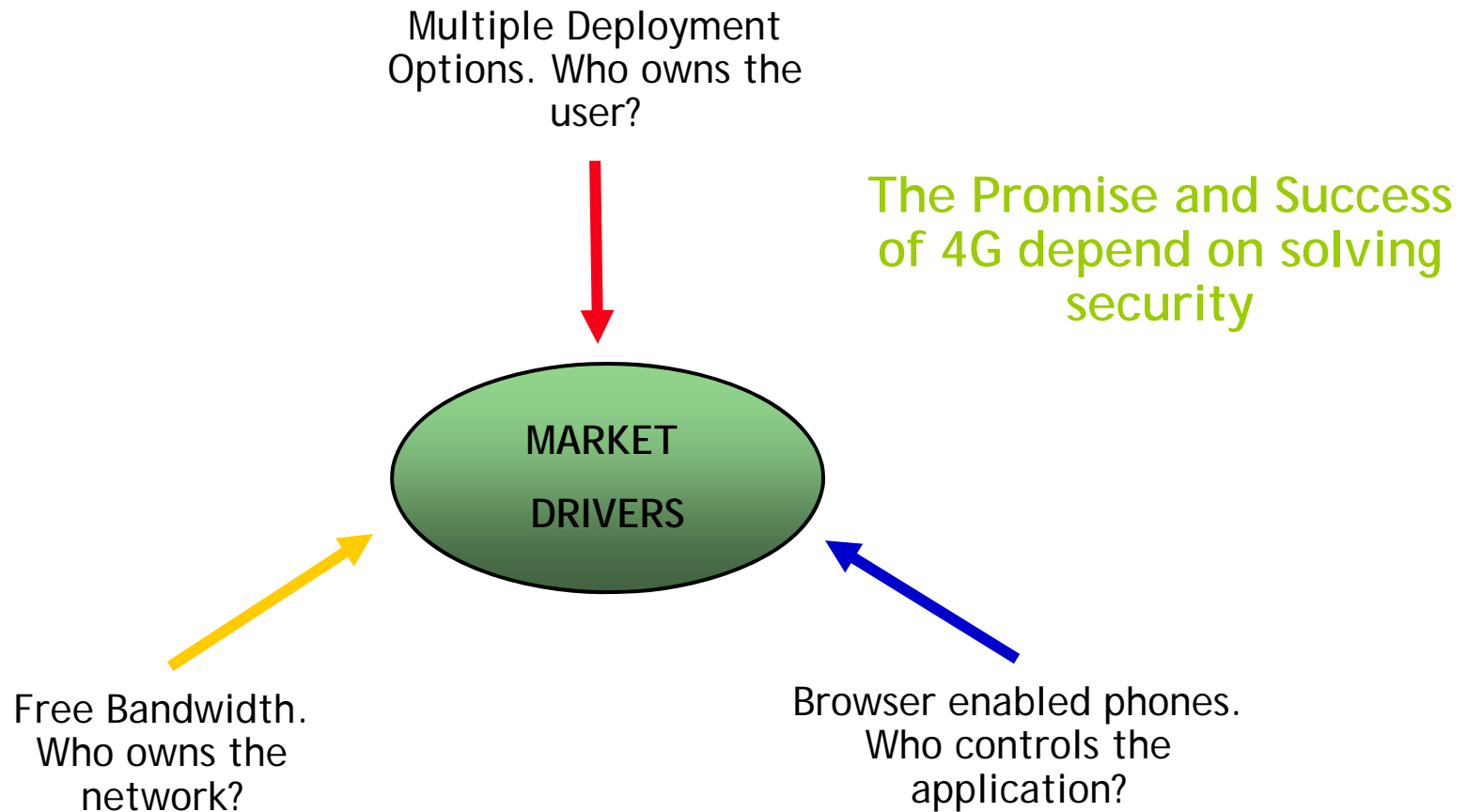
- P2P Users Download 10's of GB per day, Consuming 30% of Bandwidth

- Email Delivery Devices on average, cause 10X the Signaling Load as Phones or Aircards Used for Web-browsing

- Infected / Malfunctioning Devices Consume disproportionate amounts of Signaling Resources

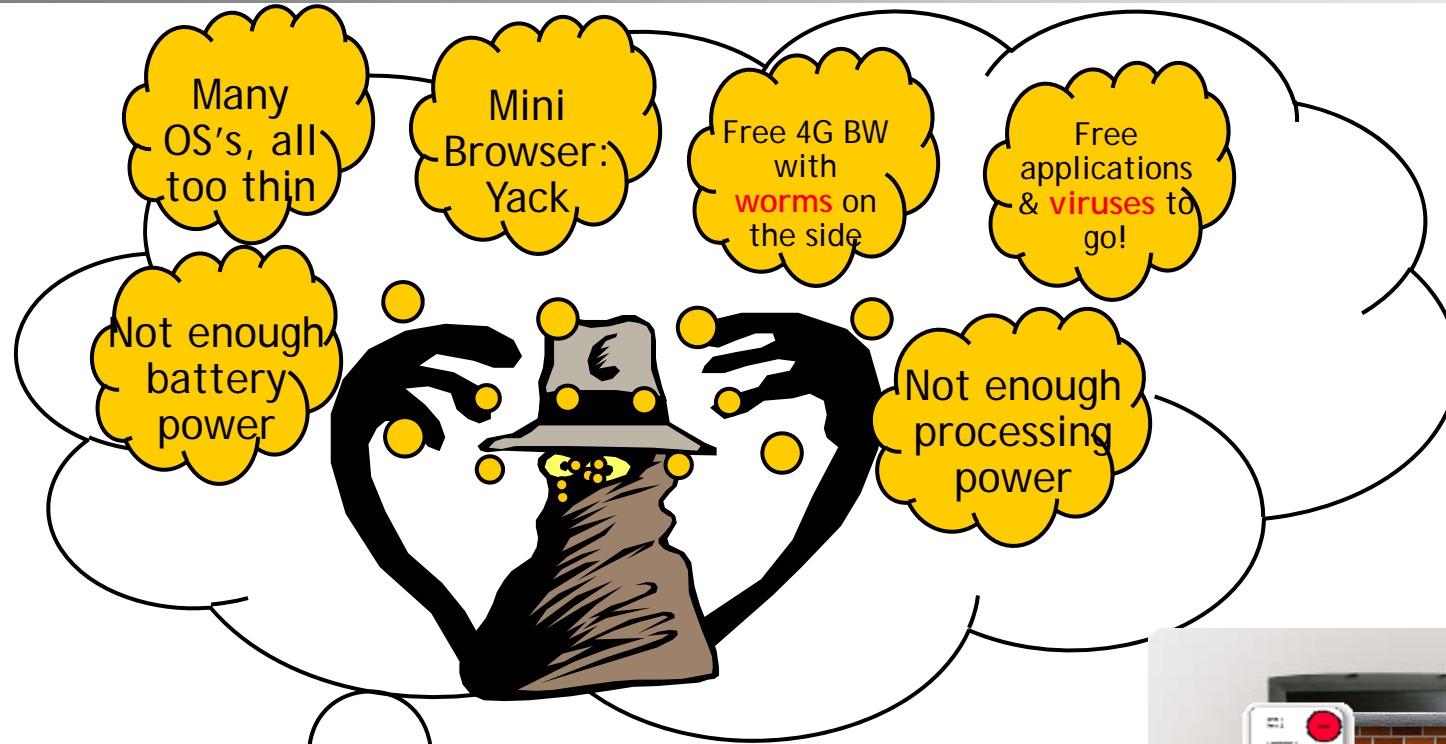
Mobile DoS: Need new tools!

Changing Business Models



New business models driving the market. What is the impact on security?

Next Gen devices: A host of challenges remain - opportunity for innovation



I have a SOLUTION



Food for thought!

Alcatel-Lucent - Leadership in Security



- **4G is about more than fat wireless pipes** - it's about creating business value - that value must be secure
 - This value can only be fully **achieved by many partners**
 - **The enterprise is no island** - a partnership in security with the service provider is vital
 - **Security is no accident** - designing for security a must
-
- Developing the **standards** - all boats float better together when interoperable
 - **Handle security in the network** so we don't replicate the horrible experience of making the end-user a security engineer
 - Developing **secure technologies** such as the NonStop Laptop Guardian and the Wireless Network Guardian to protect that valuable broadband wireless resource
 - **Creating the innovations** such as Identity Based Encryption between peers, Provable Security algorithms, efficient cryptographic protocols.
 - Exploring advantages of higher available computing power and advances in battery resources to employ **new innovative cryptographic techniques**.

www.alcatel-lucent.com

Simon Mizikovsky

smizikovsky@alcatel-lucent.com

+1-908-582-0729

+1-732-239-7533