The development of security architectures in fixed and mobile telephone systems

Lars Strand

PhD trial lecture, Ifi, UiO
22th November 2011
Oslo, Norway

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

The development of security architectures in fixed and mobile telephone systems

1) Development

2) Security architectures

A) Fixed telephone systems

B) Mobile telephone systems

The development of security architectures in fixed and mobile telephone systems

1) Development

- What are the *requirements* that we develop after?

2) Security architectures

- Establish a *definition* that meet these requirements

A) Fixed telephone systems

- Traditional “old-style” telephony (PSTN), VoIP

B) Mobile telephone systems

- GSM, 3G, LTE (4G)

“Security architecture”

- Used as a “buzzword”:
  - From cisco.com: *“To secure the new enterprise in a new world, we need a new security architecture.”*
  - From microsoft.com: *“When you understand the security architecture of Microsoft Dynamics AX, you can more easily customize security to fit the needs of your business.”*
  - From ibm.com: *“The available security product diversity in the marketplace challenges everyone in charge of designing single secure solutions or an overall enterprise security architecture.”*
- Implicit understanding or a “bag of concepts”?
  - Interpreted differently depending on who you ask
  - Often just a list of security mechanisms used within an organization
- Is there an **authoritative** definition?
  - No, according to ISSS – Information Security Society Switzerland
  - Yes, according to IETF – (their own definition from RFC4949)

Security architecture DSTO definition

"A security architecture is a high level design identifying and describing all the components used to satisfy a system's security requirements."

– Australia's Department of Defence

Security architecture OSA definition

"The design artifacts that describe how the security controls (= security countermeasures) are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system's quality attributes, among them confidentiality, integrity, availability, accountability and assurance."

– Open Security Architecture (OSA)

Security architecture OSA definition

“The design artifacts that describe how the security controls (= security countermeasures) [security mechanisms] are positioned, and how they relate to the overall IT Architecture. These controls serve the purpose to maintain the system’s quality attributes [security services], among them confidentiality, integrity, availability, accountability and assurance.”

– Open Security Architecture (OSA)

Why the diversity of meanings?

- Security architecture **for what**?
  - Organizations?
  - Products?
  - Services?
- Security architecture (in the interests) **for whom**?
  - The users (of a system)?
  - The system owners?
  - The government?

Why the diversity of meanings?

- Security architecture **for what**?
  - Organizations?
  - Products?
  - Services? → **Fixed and mobile telephony!**
- Security architecture (in the interests) **for whom**?
  - **The users (of a system)?**
  - **The system owners?**
  - **The government?**

Security architecture IETF definition

- A plan and set of principles that describe

(a) the security services that a system is required to provide to meet the needs of its users

(b) the system components required to implement the services, and

(c) the performance levels required in the components to deal with the threat environment

– RFC4949

Security architecture IETF definition

- A plan and set of principles that describe
  - (a) the security services that a system is required to provide to meet the needs of **its users**
  - (b) the system components required to implement the services, and
  - (c) the performance levels required in the components to deal with the threat environment

– RFC4949

Security architecture Template

Threats/attacks	Security services	Security mechanisms

Security architecture
Example – telephone call

Threats/attacks	Security services	Security mechanisms
A MitM attacker can eavesdrop on the call.	Confidentiality	Encryption

Public Switched Telephone Networks

- The “plain old telephone system” (with additional functionality)
- Provided (worldwide) telephone service
  - Government owned telephone companies
- Main driver telco: Availability service (postulation)
  - Limited (none?) focus on security services
  - Results in practice: No security mechanisms at all
- Stable service: 99.999% uptime
- Main driver for early attacks: Get free calls!

Attack: Blueboxing

- Signaling sent in-band
- Could be emulated and manipulated by user
- Bluebox: Dedicated devices did the work for you

Attack: Clip-on

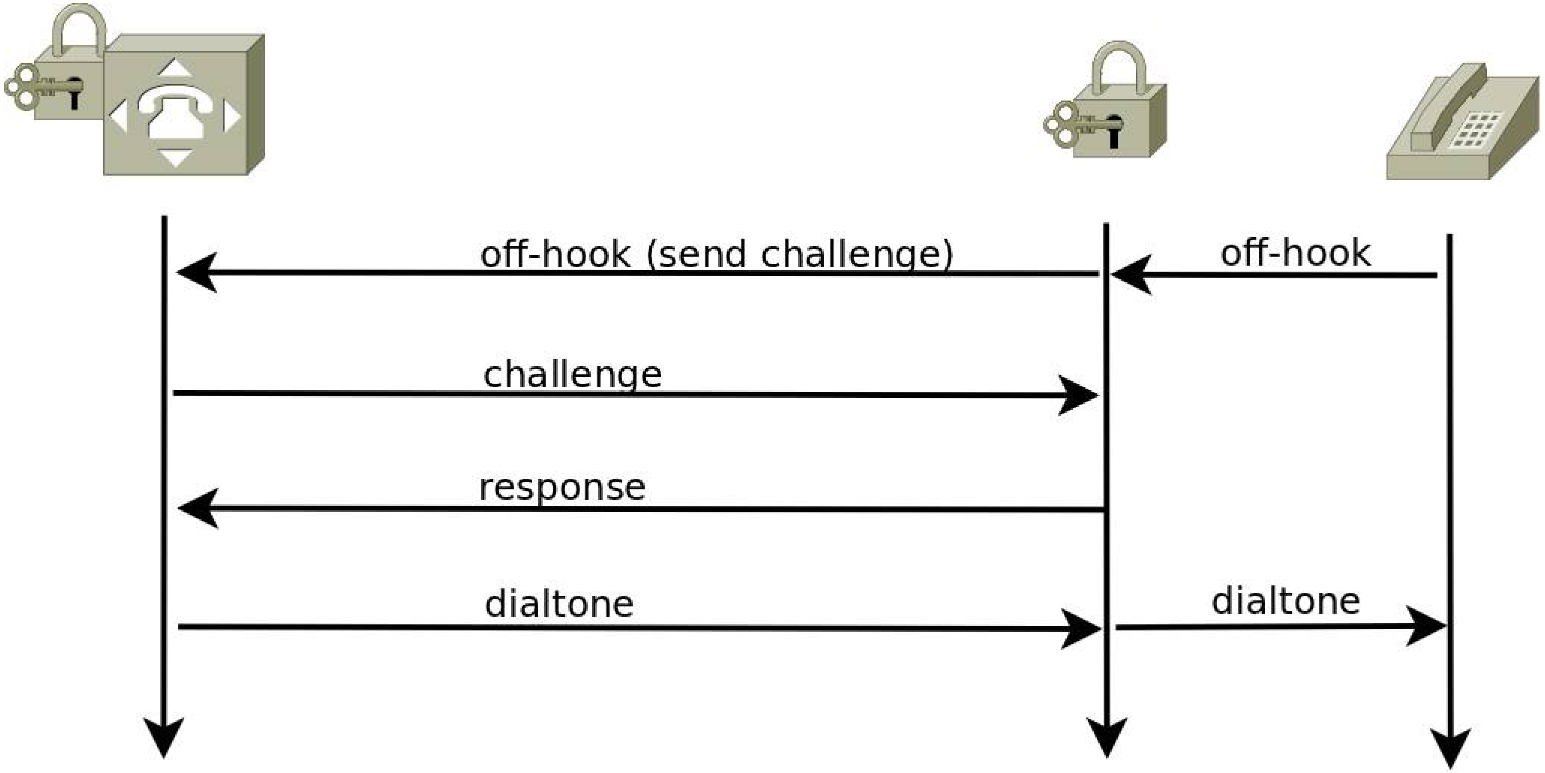
Physically attaching a phone to someone else's line to steal their service

Results:
- Customer billed incorrectly
- Hard to prove innocent

Telco incentives to follow up low:
- State owned (no competition)
- Increased usage = increased revenue (except international calls)

PSTN: Authentication

- Problem: PSTN can not distinguish between illegal and legal calls
- Vulnerability: Huge (unprotected) copper network between switching sites and customer premise
  - Some physical restriction
- Solution: Dedicated wall socket that authenticate to the access network (Jøsang, 1996)



Security architecture: PSTN

Threats/attacks	Security services	Security mechanisms
Blueboxing (inband signaling)	Access Control	Keep the signalling a secret Move signaling out-of-band
Clip-on/billing-fraud	Access Control	Authentication: Authentication Software Module, Authentication Device Restrict physical access (locks)

Conclusion: PSTN lack a decent security architecture.

Mobile systems

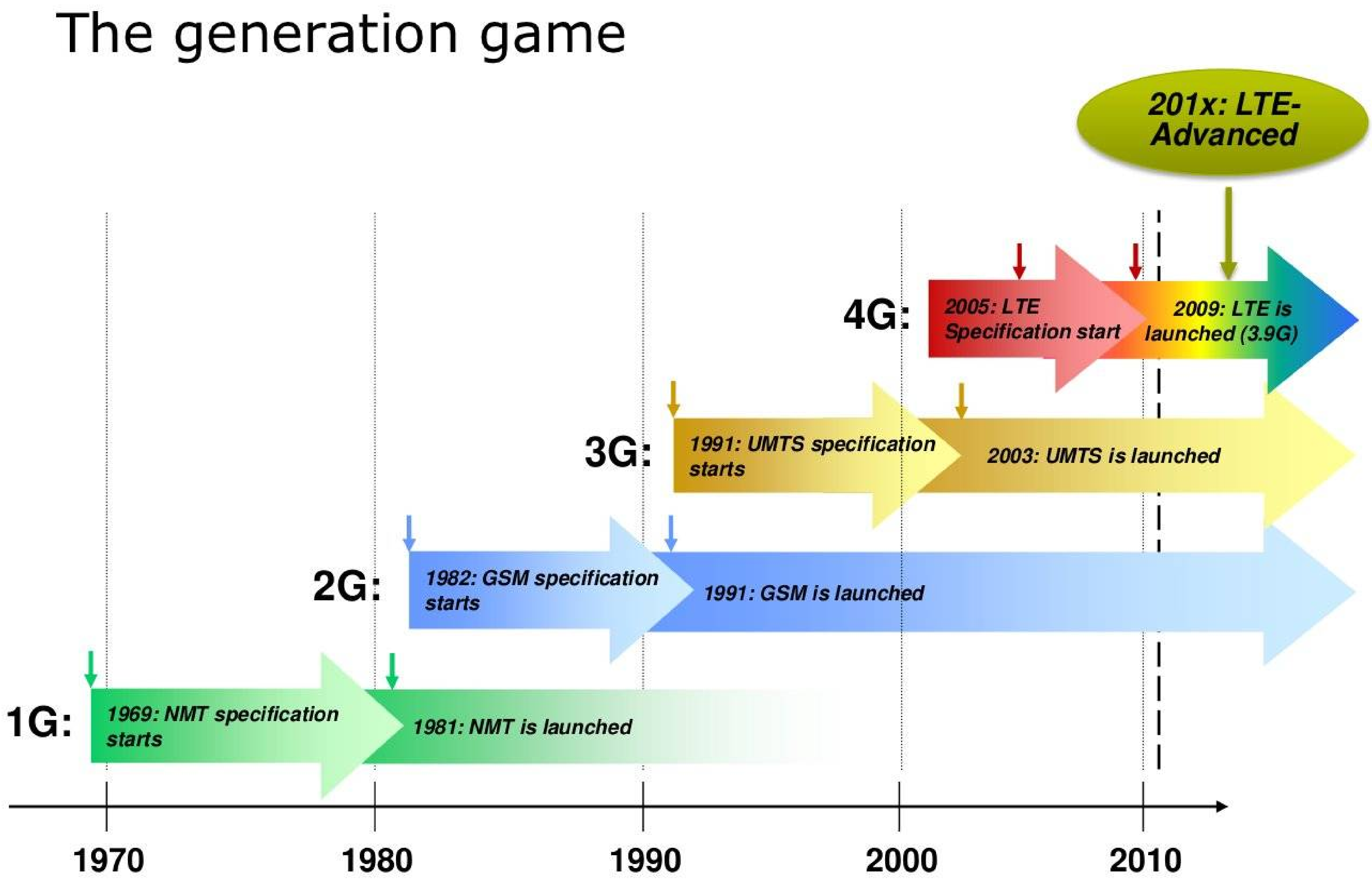

The generation game
201x: LTE-Advanced
4G:
2005: LTE Specification start
2009: LTE is launched (3.9G)
3G:
1991: UMTS specification starts
2003: UMTS is launched
2G:
1982: GSM specification starts
1991: GSM is launched
1G:
1969: NMT specification starts
1981: NMT is launched
1970
1980
1990
2000
2010

Figure from P. Lehne, Telenor

Mobile systems: GSM

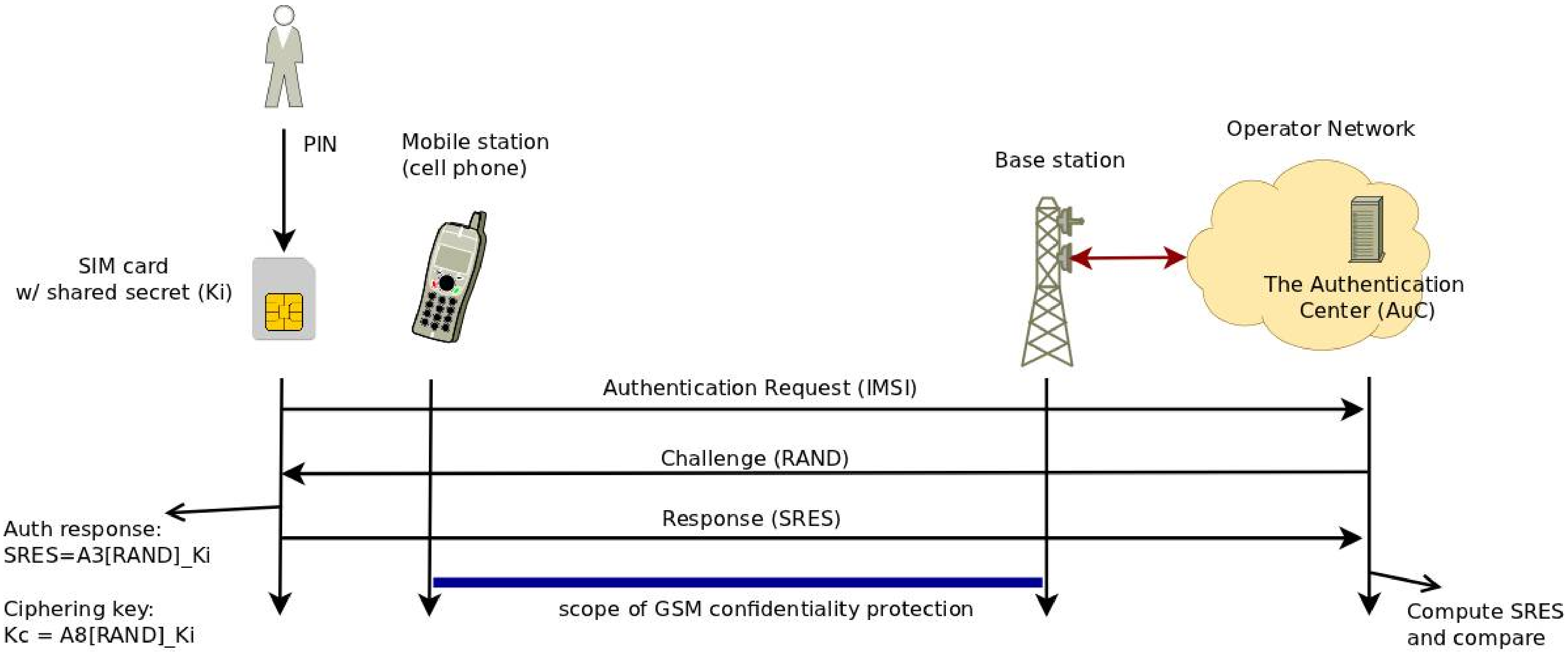
- Developed in the late 1980s, deployed 1992.
  - Norway a key developer and inventor
- Today: Cover 80% of world population (5+ billion users!), gsmworld.com.
- GSM security goal: “as secure as the wire”
- GSM network consists of several network elements
  - Radio Subsystem (RSS)
    - Base station Subsystem (BSS)
    - Mobile Equipment (ME) (cell phone/handset)
  - Network and Switching Subsystem (NSS) – core network
  - Operation Subsystem (OSS)

Threat environment

1. Vulnerability: Cloning
   - GSM security service: Authentication
   - GSM security mechanism: Authentication mechanism
2. Vulnerability: Content (voice) sent in clear
   - GSM security service: Call content confidentiality
   - GSM security mechanism: A5/1, A5/2, A5/3, A5/4
3. Vulnerability: Spying (subscriber location tracking)
   - GSM security service: Identity confidentiality
   - GSM security mechanism: Location security (TMSI)

GSM authentication

Authentication mechanism performed using a challenge-response
- Shared secret between SIM card and AuC



GSM: Problems

- Focus on *access security*
  - Confidentiality terminated at the base stations
  - Weak operator network protection
  - Example: Traffic to/from BS and AuC should be protected!
- *"Security through obscurity"* - A3/A5/A8 eventually leaked
- Algorithms not resistant to cryptanalysis attack
  - A5/1 can "easily" be broken – today gradually replaced by A5/3
  - No public scrutiny during development
- Lack of user visibility
  - User do not know if/what encryption is used
- Difficult to upgrade cryptographic algorithms
  - But not in theory? Resides on the SIM card
- Authentication: One-way authentication only
  - Only MS to BS and not BS to MS.
- + many more..

Security architecture: GSM

Threats/attacks	Security services	Security mechanisms
Cloning	Authentication	Authentication mechanism (challenge-response with a shared secret)
Eavesdropping (voice sent in clear)	Confidentiality	Encryption of call content (A5/1, A5/2, A5/3)
Spying (identity tracking)	Confidentiality	Location security (TMSI)

Conclusion: GSM had a security architecture from the start

* Well defined threats and security services (at the time)

* Security mechanisms implemented poorly

- missing public scrutiny
- hard to replace components
- not adaptive to future changes

Mobile systems: 3GPP

- Third generation partnership project (3GPP)
  - Structured in releases – latest is v11 published sept 2011
- Today: Replacing GSM world-wide
- Includes mobile technologies like:
  - UMTS (3G) – Deployed by Telenor in 2001
  - LTE (not 4G) – Deployed by Netcom in 2010, Telenor in 2012.
  - LTE Advanced (4G) – specification ready 2011Q1
- Building on and evolved from GSM
  - Early goal: Access architecture should be compatible with GSM
  - Backward compatible with a system with weaker security is undesirable – but commercial reality dictated otherwise

UMTS (3G)

- Universal Mobile Telecommunications System (UMTS)
- Security mechanisms in GSM used as starting point for UMTS
- UMTS objectives, specified in *3G TS 33.120, 3G Security, Security Principles and Objectives*:
  - UTMS security will **build on** the security of 2G systems
  - UMTS security will **improve** on the security of 2G systems
  - UTMS security will **offer new** security features [services]
- Threat/risk analysis for 3G systems performed
  - *3G TS 21.133, 3G Security, Security Threats and Requirements*
- The objectives + threat environment became basis for
  - *3G TS 33.102, 3G Security, Security Architecture*

Security architecture: UMTS

Main tasks of the security architecture (Køien, 2004):

1) Authentication
   - GSM vulnerability: False BST
   - UMTS: Mutual authentication, new algorithm (MILENAGE)
2) Replace algorithms/New key generation
   - GSM vulnerability: Inadequate algorithm
   - UMTS: New algorithm (KASUMI)
3) Encryption/integrity protection
   - GSM vulnerability: Cipher keys and auth data sent in clear in operator network
   - UMTS: Extend confidentiality and integrity service to the operator network

Security architecture: UMTS

Threats/attacks	Security services	Security mechanisms
False BST	Authentication	Mutual authentication mechanism (challenge-response with a shared secret)
Eavesdropping (Poor GSM encryption)	Confidentiality	Encryption of signaling and call content
Data sent in clear in the operator network	Confidentiality	Encryption and integrity protection of data, to also cover operator network

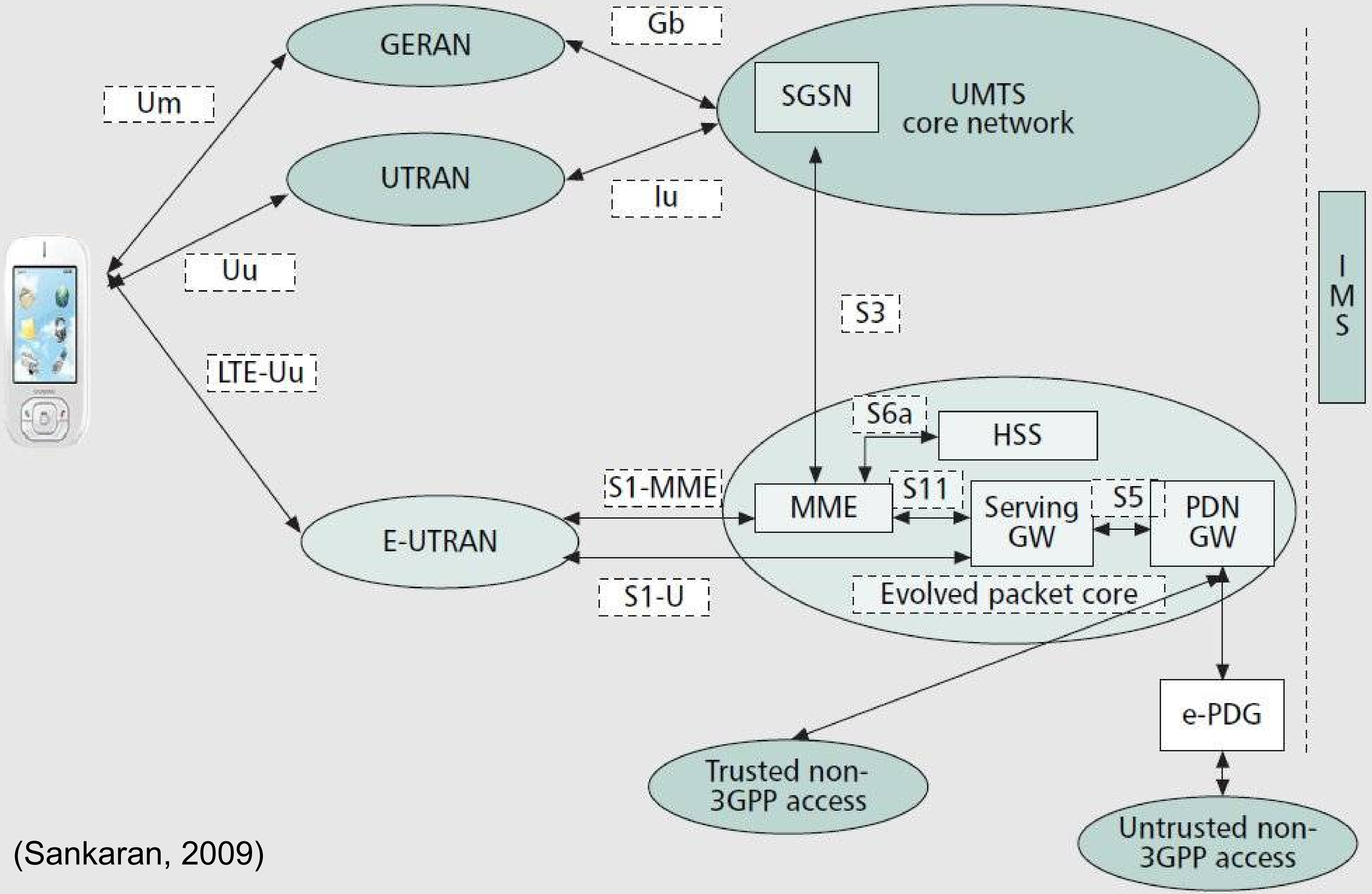
Conclusion: UMTS has a decent security architecture

* Extensive threat and attack analysis
* Open development
* Modular ("flexible") security mechanisms
  - "cryptographic core" can be replaced by operator
* Target: End-user, Operators and law enforcements

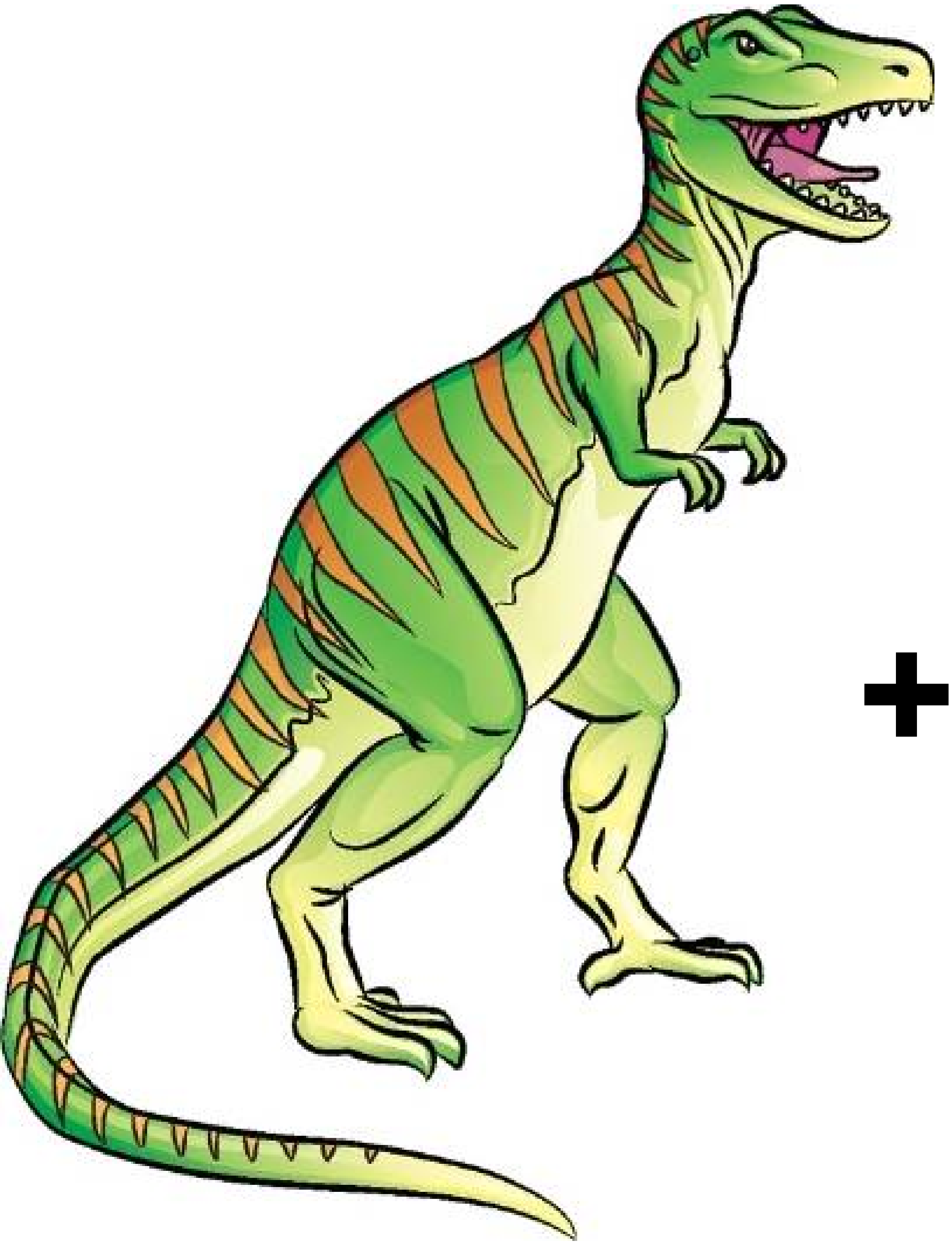
LTE Advanced (4G)

- Long Term Evolution/System Architecture Evolution (LTE/SAE)
- Overall architecture of Evolved Packet System (EPS) consists of:
    1) Access network
    2) Evolved Packet Core (EPC) network
        - IP Multimedia Subsystem (IMS)
- *“Improved overall security robustness over UMTS”*
- Major changes from UMTS:
    - All IP network (AIPN)
    - Higher bandwidth
    - May use non-3GPP access networks

LTE: EPS architecture



(Sankaran, 2009)



+

KISS?

LTE: Heterogeneous networks

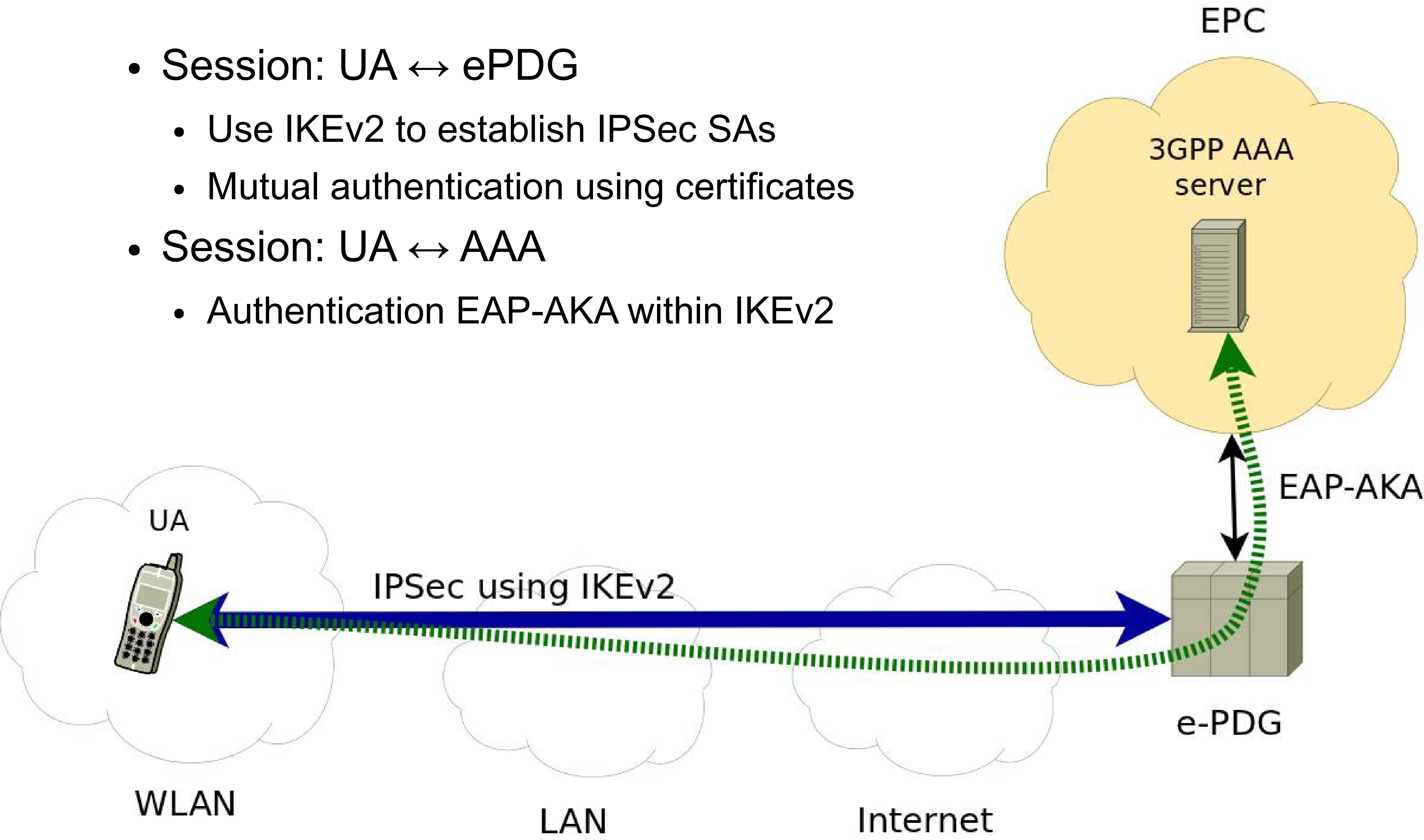
- Non-3GPP access network include:
  - cdm2000, WiFi (WLAN), fixed networks (Internet)
- Two classes of network access defined:

1) Trusted access – has direct access to the operator network
   - Network operator decide which access technology is trusted
   - Can use EAP-AKA

2) Untrusted access – everything else
   - Require IPSec with IKEv2 + EAP-AKA
   - Challenges: New threats (Internet), performance!

LTE: Non-3GPP untrusted access

- Session: UA ↔ ePDG
  - Use IKEv2 to establish IPSec SAs
  - Mutual authentication using certificates
- Session: UA ↔ AAA
  - Authentication EAP-AKA within IKEv2



Security architecture: LTE

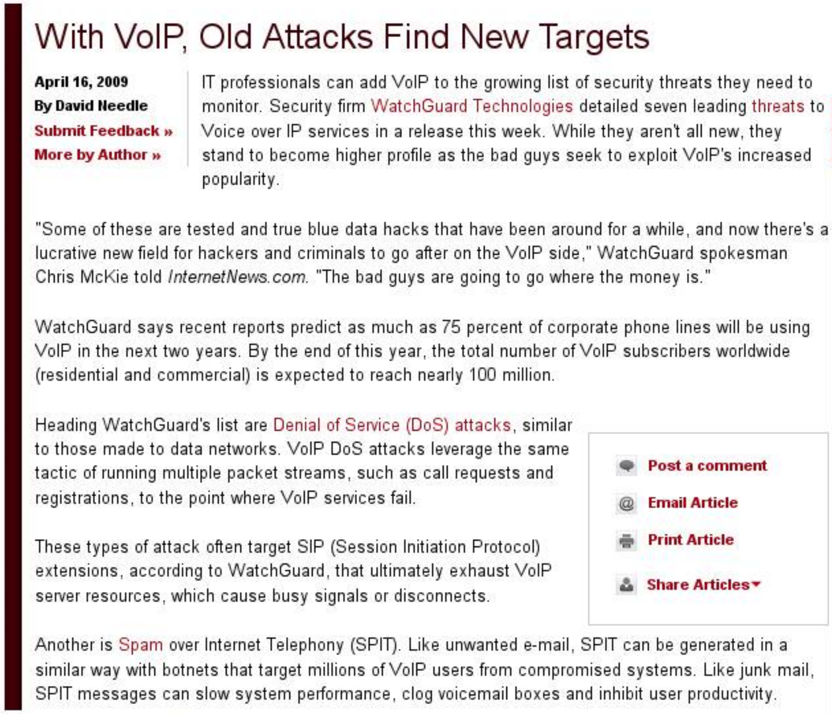
Threats/attacks	Security services	Security mechanisms
Eavesdropping	Data confidentiality	IPSec
Modification of content	Data integrity	IPSec
Impersonation	Authentication	EAP-AKA
Denial of service, roaming, performance	Availability service	?, fast re-authentication? different access network?

Conclusion: LTE has a decent security architecture

* Built on and improved over UMTS
* All-IP architecture a challenge
* Untrusted non-3GPP access a challenge
* Performance might be an issue

Voice over IP

- VoIP is here to stay
  - Cheaper (both communication and operational costs)
  - More functionality (video, HD sound, presence, IM, ..)
  - High industry focus
- VoIP loaded with security challenges
  - Inherit (traditional) packet switched network security problems, and..
  - Introduces new ones (because of “new” technology)



With VoIP, Old Attacks Find New Targets

April 16, 2009
By David Needle
Submit Feedback »
More by Author »

IT professionals can add VoIP to the growing list of security threats they need to monitor. Security firm WatchGuard Technologies detailed seven leading threats to Voice over IP services in a release this week. While they aren't all new, they stand to become higher profile as the bad guys seek to exploit VoIP's increased popularity.

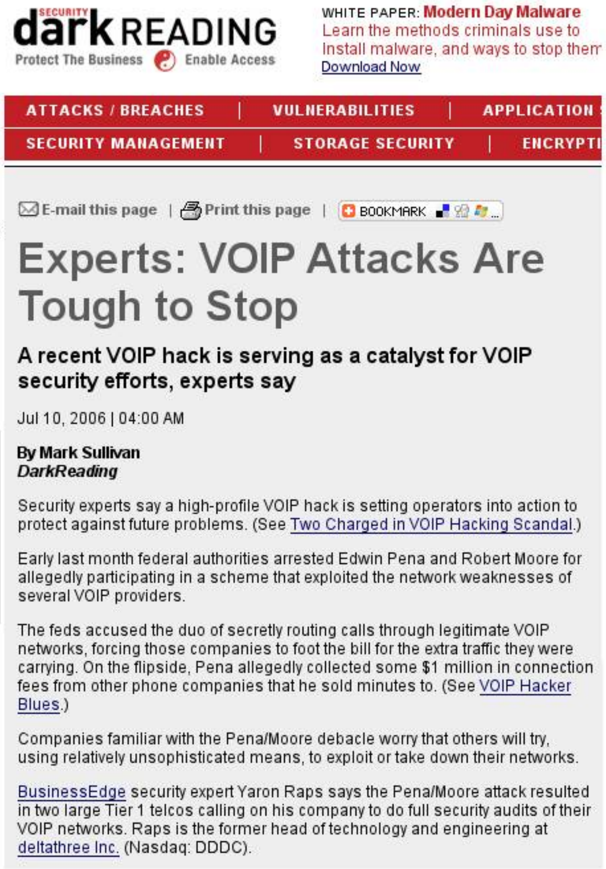
"Some of these are tested and true blue data hacks that have been around for a while, and now there's a lucrative new field for hackers and criminals to go after on the VoIP side," WatchGuard spokesman Chris McKie told *InternetNews.com*. "The bad guys are going to go where the money is."

WatchGuard says recent reports predict as much as 75 percent of corporate phone lines will be using VoIP in the next two years. By the end of this year, the total number of VoIP subscribers worldwide (residential and commercial) is expected to reach nearly 100 million.

Heading WatchGuard's list are Denial of Service (DoS) attacks, similar to those made to data networks. VoIP DoS attacks leverage the same tactic of running multiple packet streams, such as call requests and registrations, to the point where VoIP services fail.

These types of attack often target SIP (Session Initiation Protocol) extensions, according to WatchGuard, that ultimately exhaust VoIP server resources, which cause busy signals or disconnects.

Another is Spam over Internet Telephony (SPIT). Like unwanted e-mail, SPIT can be generated in a similar way with botnets that target millions of VoIP users from compromised systems. Like junk mail, SPIT messages can slow system performance, clog voicemail boxes and inhibit user productivity.



dark READING
Protect The Business Enable Access
ATTACKS / BREACHES | VULNERABILITIES | APPLICATION S
SECURITY MANAGEMENT | STORAGE SECURITY | ENCRYPTI
E-mail this page | Print this page | BOOKMARK

Experts: VOIP Attacks Are Tough to Stop

A recent VOIP hack is serving as a catalyst for VOIP security efforts, experts say

Jul 10, 2006 | 04:00 AM

By Mark Sullivan
DarkReading

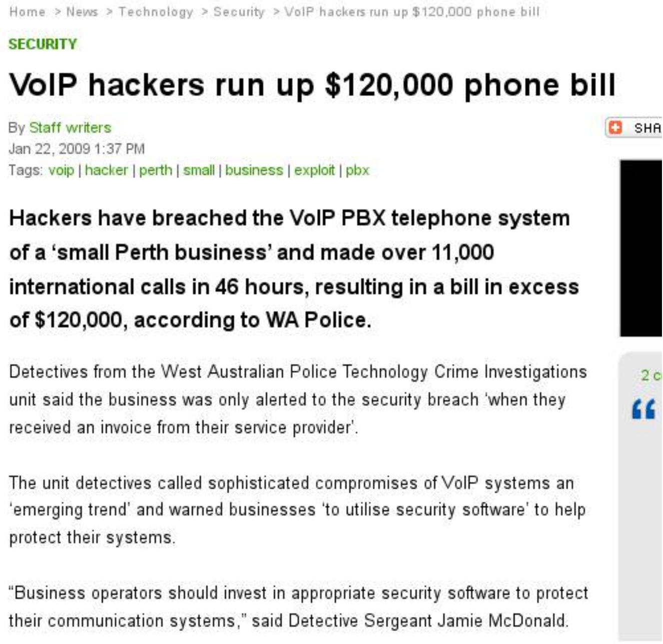
Security experts say a high-profile VOIP hack is setting operators into action to protect against future problems. (See Two Charged in VOIP Hacking Scandal.)

Early last month federal authorities arrested Edwin Pena and Robert Moore for allegedly participating in a scheme that exploited the network weaknesses of several VOIP providers.

The feds accused the duo of secretly routing calls through legitimate VOIP networks, forcing those companies to foot the bill for the extra traffic they were carrying. On the flipside, Pena allegedly collected some $1 million in connection fees from other phone companies that he sold minutes to. (See VOIP Hacker Blues.)

Companies familiar with the Pena/Moore debacle worry that others will try, using relatively unsophisticated means, to exploit or take down their networks.

BusinessEdge security expert Yaron Raps says the Pena/Moore attack resulted in two large Tier 1 telcos calling on his company to do full security audits of their VOIP networks. Raps is the former head of technology and engineering at deltathree Inc. (Nasdaq: DDDC).



Home > News > Technology > Security > VoIP hackers run up $120,000 phone bill
SHA
2 c

SECURITY

VoIP hackers run up $120,000 phone bill

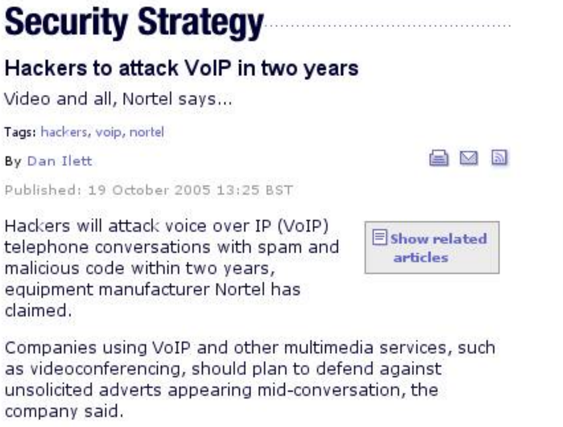
By Staff writers
Jan 22, 2009 1:37 PM
Tags: voip | hacker | perth | small | business | exploit | pbx

Hackers have breached the VoIP PBX telephone system of a 'small Perth business' and made over 11,000 international calls in 46 hours, resulting in a bill in excess of $120,000, according to WA Police.

Detectives from the West Australian Police Technology Crime Investigations unit said the business was only alerted to the security breach 'when they received an invoice from their service provider'.

The unit detectives called sophisticated compromises of VoIP systems an 'emerging trend' and warned businesses 'to utilise security software' to help protect their systems.

"Business operators should invest in appropriate security software to protect their communication systems," said Detective Sergeant Jamie McDonald.



Security Strategy

Hackers to attack VoIP in two years

Video and all, Nortel says...

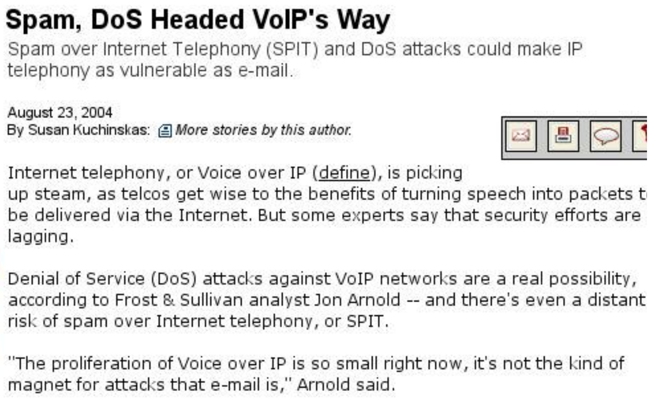
Tags: hackers, voip, nortel

By Dan Ilett

Published: 19 October 2005 13:25 BST

Hackers will attack voice over IP (VoIP) telephone conversations with spam and malicious code within two years, equipment manufacturer Nortel has claimed.

Companies using VoIP and other multimedia services, such as videoconferencing, should plan to defend against unsolicited adverts appearing mid-conversation, the company said.



Spam, DoS Headed VoIP's Way

Spam over Internet Telephony (SPIT) and DoS attacks could make IP telephony as vulnerable as e-mail.

August 23, 2004
By Susan Kuchinskas: *More stories by this author.*

Internet telephony, or Voice over IP (define), is picking up steam, as telcos get wise to the benefits of turning speech into packets t be delivered via the Internet. But some experts say that security efforts are lagging.

Denial of Service (DoS) attacks against VoIP networks are a real possibility, according to Frost & Sullivan analyst Jon Arnold -- and there's even a distant risk of spam over Internet telephony, or SPIT.

"The proliferation of Voice over IP is so small right now, it's not the kind of magnet for attacks that e-mail is," Arnold said.

SANS Top-20 2007 Security Risks (2007 Annual Update)

For a continuous update on the SANS Top 20 vulnerabilities, subscribe to @Risk. If y
Summary pointing out newsworthy highlights of the SANS 2007 Top Internet Se

ıerabilities in:

nerabilities in:

s
Services
re
vers
e

Security Policy and

H1. Excessive User Rights a
H2. Phishing/Spear Phishing
H3. Unencrypted Laptops a

Application Abuse:

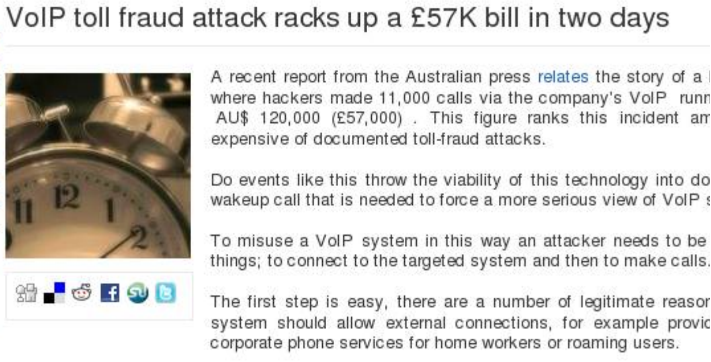
A1. Instant Messaging
A2. Peer-to-Peer Programs

Network Devices:

N1. VoIP Servers and Phones

Zero Day Attacks:

Z1. Zero Day Attacks



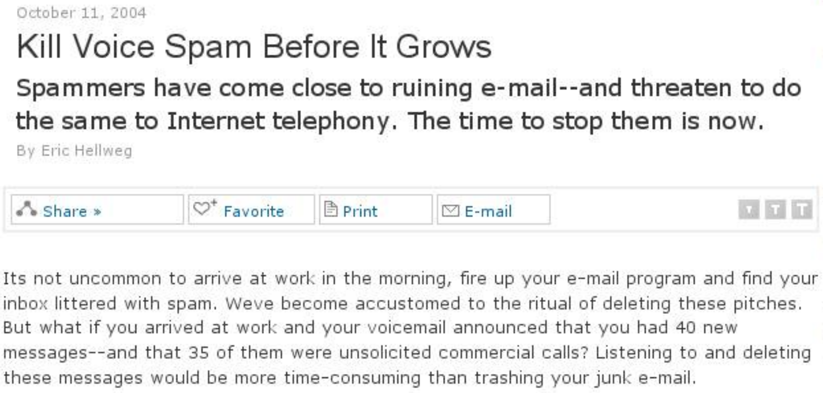
VoIP toll fraud attack racks up a £57K bill in two days

A recent report from the Australian press relates the story of a where hackers made 11,000 calls via the company's VoIP runn AU$ 120,000 (£57,000) . This figure ranks this incident am expensive of documented toll-fraud attacks.

Do events like this throw the viability of this technology into do wakeup call that is needed to force a more serious view of VoIP s

To misuse a VoIP system in this way an attacker needs to be things; to connect to the targeted system and then to make calls.

The first step is easy, there are a number of legitimate reasor system should allow external connections, for example provic corporate phone services for home workers or roaming users.



October 11, 2004

Kill Voice Spam Before It Grows

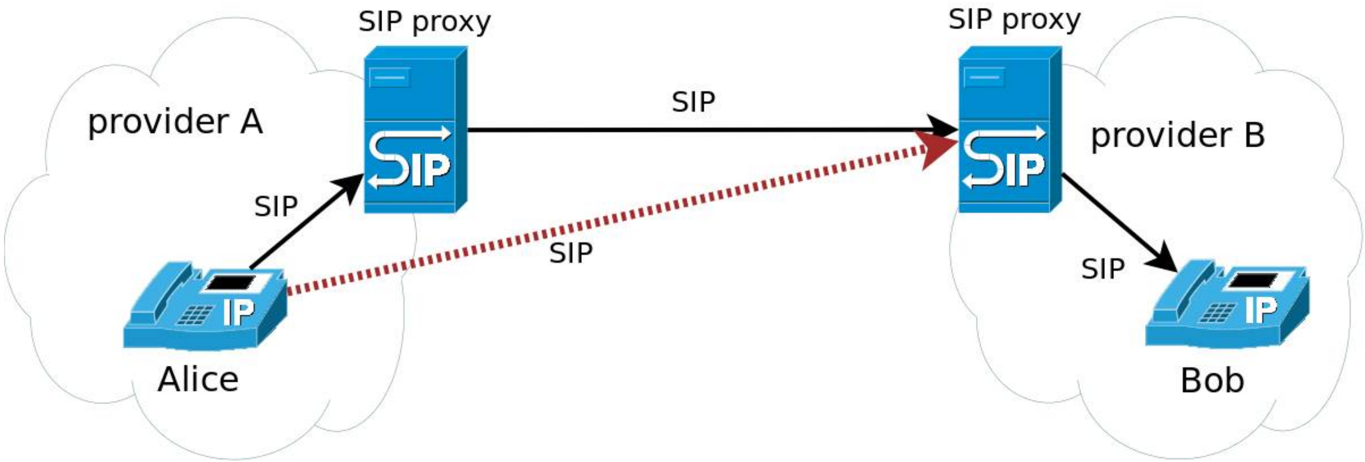
Spammers have come close to ruining e-mail--and threaten to do the same to Internet telephony. The time to stop them is now.

By Eric Hellweg

Its not uncommon to arrive at work in the morning, fire up your e-mail program and find your inbox littered with spam. Weve become accustomed to the ritual of deleting these pitches. But what if you arrived at work and your voicemail announced that you had 40 new messages--and that 35 of them were unsolicited commercial calls? Listening to and deleting these messages would be more time-consuming than trashing your junk e-mail.

VoIP threats

1. Hard to assure the identity of the caller



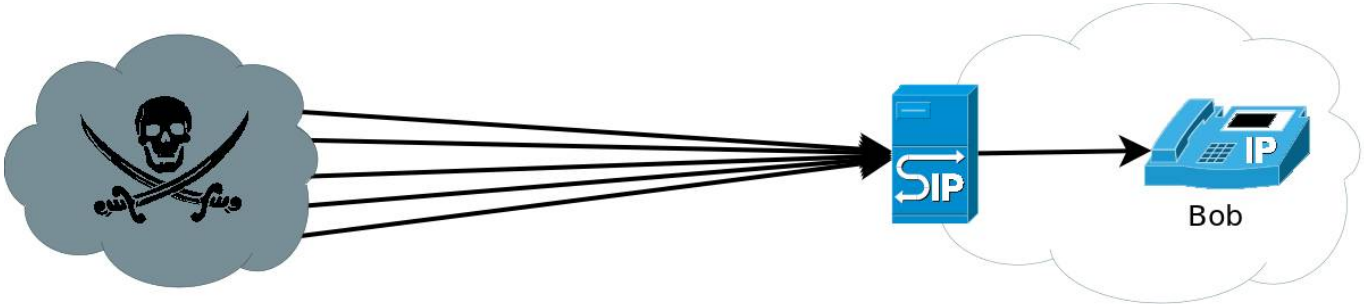
2. SPam over Internet Telephony (SPIT)

- **Hard: Unknown attack vector**
- **Worse than SPAM**
- **How to mitigate: SPIDER, RFC 5039**

VoIP threats

3. Denial of Service (DoS)

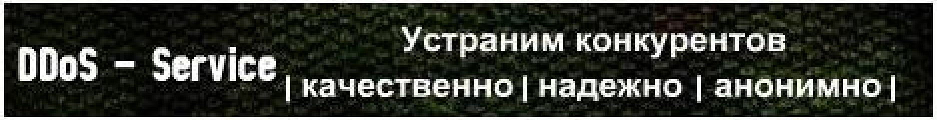
- Simple and effective: Send more bogus traffic than the recipient can handle
- No easy fix to prevent



Example: DDoS for sale - The ad scrolls through several messages, including

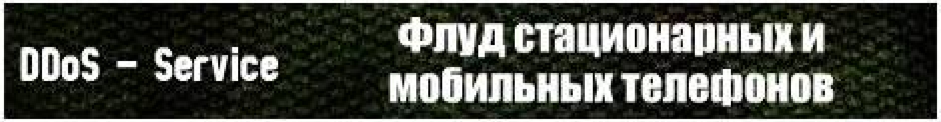
- "Will eliminate competition: high-quality, reliable, anonymous."
- "Flooding of stationary and mobile phones."
- "Pleasant prices: 24-hours start at $80. Regular clients receive significant discounts."
- "Complete paralysis of your competitor/foe."

Reference: http://isc.sans.org/diary.html?storyid=5380



DDoS - Service

Устраним конкурентов
| качественно | надежно | анонимно |



DDoS - Service

Флуд стационарных и
мобильных телефонов

Security architecture: VoIP

Threats/attacks	Security services	Security mechanisms
Identity fraud	Authentication Access Control	Authentication mechanism Access lists, SIP Peering
SPIT	Authentication Access Control	Authentication mechanisms White- and blacklists
Denial of Service	Availability	No easy fix

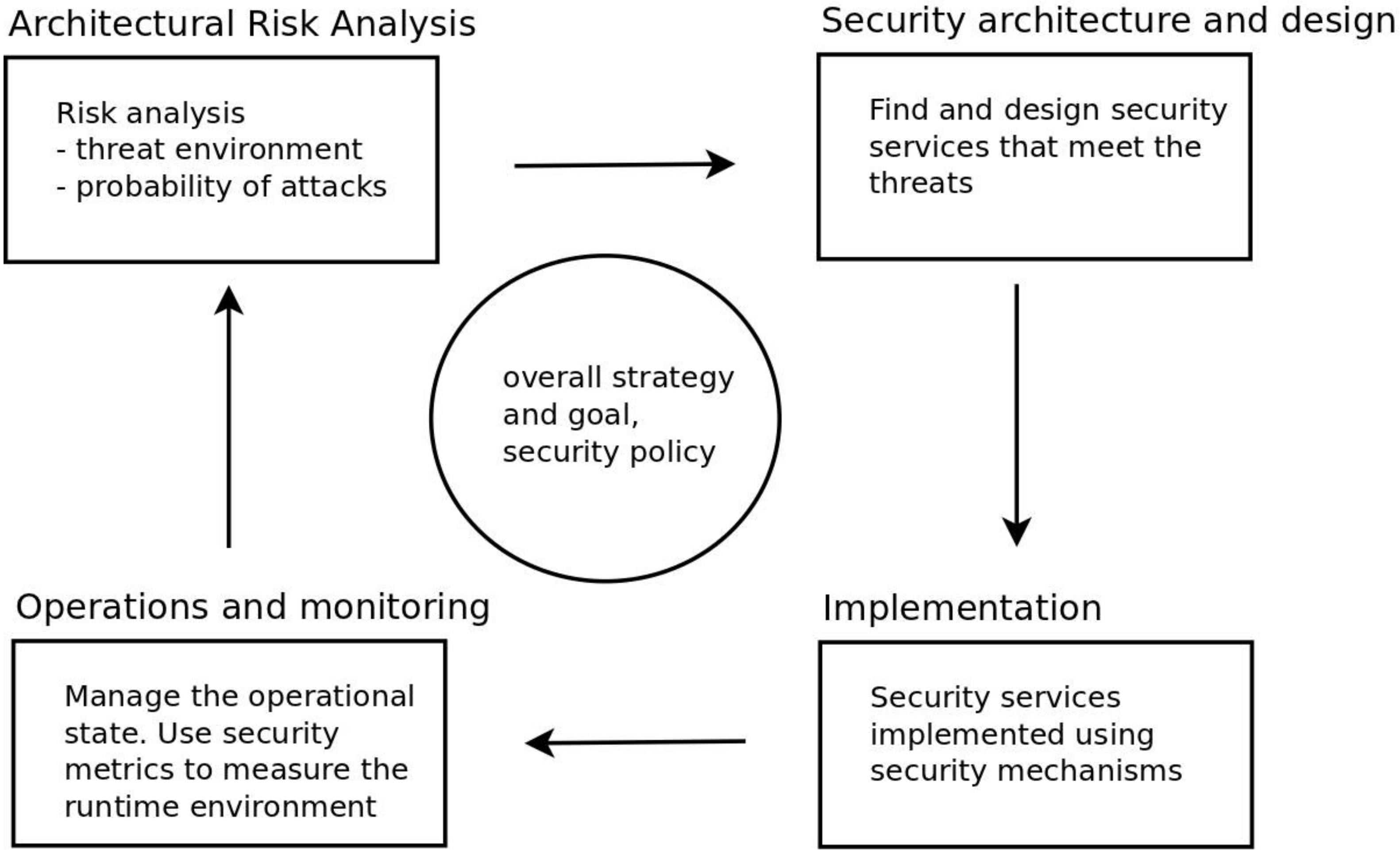
Conclusion: No decent security architecture

* Re-engineering protocols to adapt to new security mechanisms

* VoIP systems usually “shielded in”

Security architecture - revisited

- Security architecture is a “iterative process” – Peterson, 2006:



Architectural Risk Analysis

Risk analysis
- threat environment
- probability of attacks

Security architecture and design

Find and design security services that meet the threats

overall strategy and goal, security policy

Operations and monitoring

Manage the operational state. Use security metrics to measure the runtime environment

Implementation

Security services implemented using security mechanisms

Closing remarks

Some lessons when developing a security architecture for telephony:

- There is no “single security architecture” that works for all
  - iterative process, technology dependent
- A security architecture should be able to adapt to changes in the threat environment
- Do a proper risk/threat analysis – get to know the “lay of the land”
- Open development → public scrutiny
- Use well-established/open standards where possible (do not “re-invent the wheel”)

- Conclusion: Mobile telephony systems has done a better job to develop a security architecture than fixed telephony (VoIP).

References: Security architecture

- Gunnar Peterson. *“Security Architecture Blueprint”*, Arctec Group, 2006 (Whitepaper)
- Information Security Society Switzerland (ISSS), *“What is a Security Architecture”*, WG Security Architecture, 2008
- Robert Shirey. *“RFC4949: Internet Security Glossary, Version 2”*, August 2007, http://tools.ietf.org/html/rfc4949.
- Suhair Hafez Amer and John A. Hamilton, Jr. *“Understanding security architecture”,* in Proceedings of the 2008 Spring simulation multiconference, SpringSim ’08 (San Diego, CA, USA: Society for Computer Simulation International, 2008), 335–342
- The Defence Science and Technology Organisation (DSTO), *“A Survey of Techniques for Security Architecture Analysis”*, Technical Report DSTO-TR-1438, Department of Defence, Australia, 2003

References: Fixed telephony

- Audun Jøsang and Knut Johannessen. *“Authentication in Analogue Telephone Access Networks”*, in Prageocrypt 96, ISBN: 80-01-01502-5; pp 324-336.
- D. Richard Kuhn. “Sources of Failure in the Public Switched Telephone Network”, Computer, 30:31-36, 1997
- Iosif Androulidakis. *“On the importance of securing telephony systems”*. WSEAS transaction on communications, issue 1, vol 8, ISSN: 1109-2742, Jan 2009
- Ron Rosenbaum. *“The Official Phreaker's Manual”*. Esquire Magazine, Oct 1971.
- Ross Anderson. Chapter 20 in *“Security Engineering”*. 2nd edition, Wiley, 2008.
- H. Sinnreich and A. B. Johnston. “Internet Communications using SIP: Delivering VoIP and multimedia services with Session Initiation Protocol”, 2nd edition, Wiley, August 2006
- Sisalem, et al. “SIP Security”, WileyBlackwell, 2009.
- Lars Strand and Wolfgang Leister. *“A Survey of SIP Peering”*, In NATO ASI – Architects of secure Networks (ASIGE10), May 2010
- Lars Strand and Wolfgang Leister. *“Advancement towards secure authentication in the session initiation protocol”*, Submitted to International Journal on Advances in Security, 2011.

References: Mobile telephony

- 3GPP TS 21.133 v4.1.0 “3G Security; Security Threats and Requirements”, at http://www.3gpp.org/ftp/Specs/html-info/33133.htm
- 3GPP TS 33.120 v4.0.0 “3G Security; Security principles and objectives”, at http://www.3gpp.org/ftp/Specs/html-info/33120.htm
- 3GPP TS 33.402 v11.1.0 “3GPP System Archtiecture Evolution (SAE); Security aspect of non-3GPP accesses”, at http://www.3gpp.org/ftp/Specs/html-info/33402.htm
- 3GPP TS 33.102 v11.0.0 *“3G Security; Security Architecture”*, at http://www.3gpp.org/ftp/Specs/html-info/33102.htm
- C.B. Sankaran. "Network access security in next- generation 3GPP systems: A tutorial", IEEE Comm.magazine, February 2009
- David Margrave. *“GSM Security and Encryption”*, George Mason University, (Whitepaper)
- Geir Køien, *"An introduction to access security in UMTS"*, IEEE Wireless Comm.magazine, February, 2004
- Geir Køien and Thomas Haslestad. *“Security Aspects of 3G-WLAN Interworking”*, IEEE Communications Magazine, ISSN 0163-6804, November 2003, Vol.41, No.11, pp82-88, November 2003
- Geir Køien, *"Access Security in 3GPP-based Mobile Broadband Systems"*, Telektronikk, 2010

Thank you!