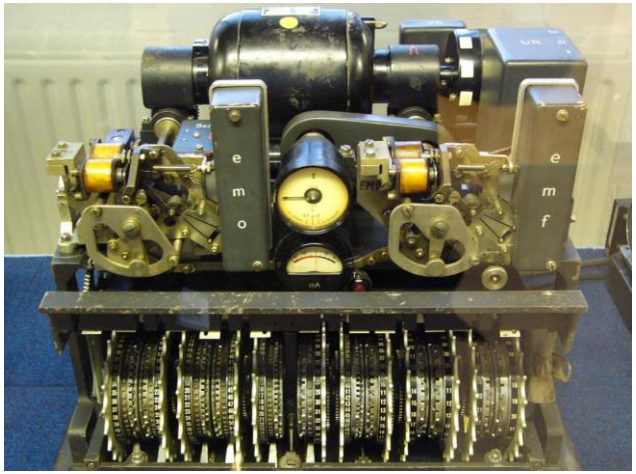
CONNECTION SECURITY



The German Lorenz SZ42 Cipher Machine at the National Museum of Computing (TNMOC), Bletchley Park, UK. The SZ42 was used by the German High Command in the early 1940s to encrypt telecommunication messages during World War II.

Contents

Part I

- Crypto applied
  - Choice of algos
  - Object security
  - Perfect Forward Secrecy
  - Opportunistic encryption
  - Forward/Backward security

Part II

- Access
  - Triple A (AAA)
    - CHAP, EAP
    - Radius, Diameter
  - SSO, FID
  - GBA

Part III

- Secure connections
  - Internet encryption
  - TLS, DTLS
  - IPSEC
  - Internet of Things (IoT)
  - GSM, LTE

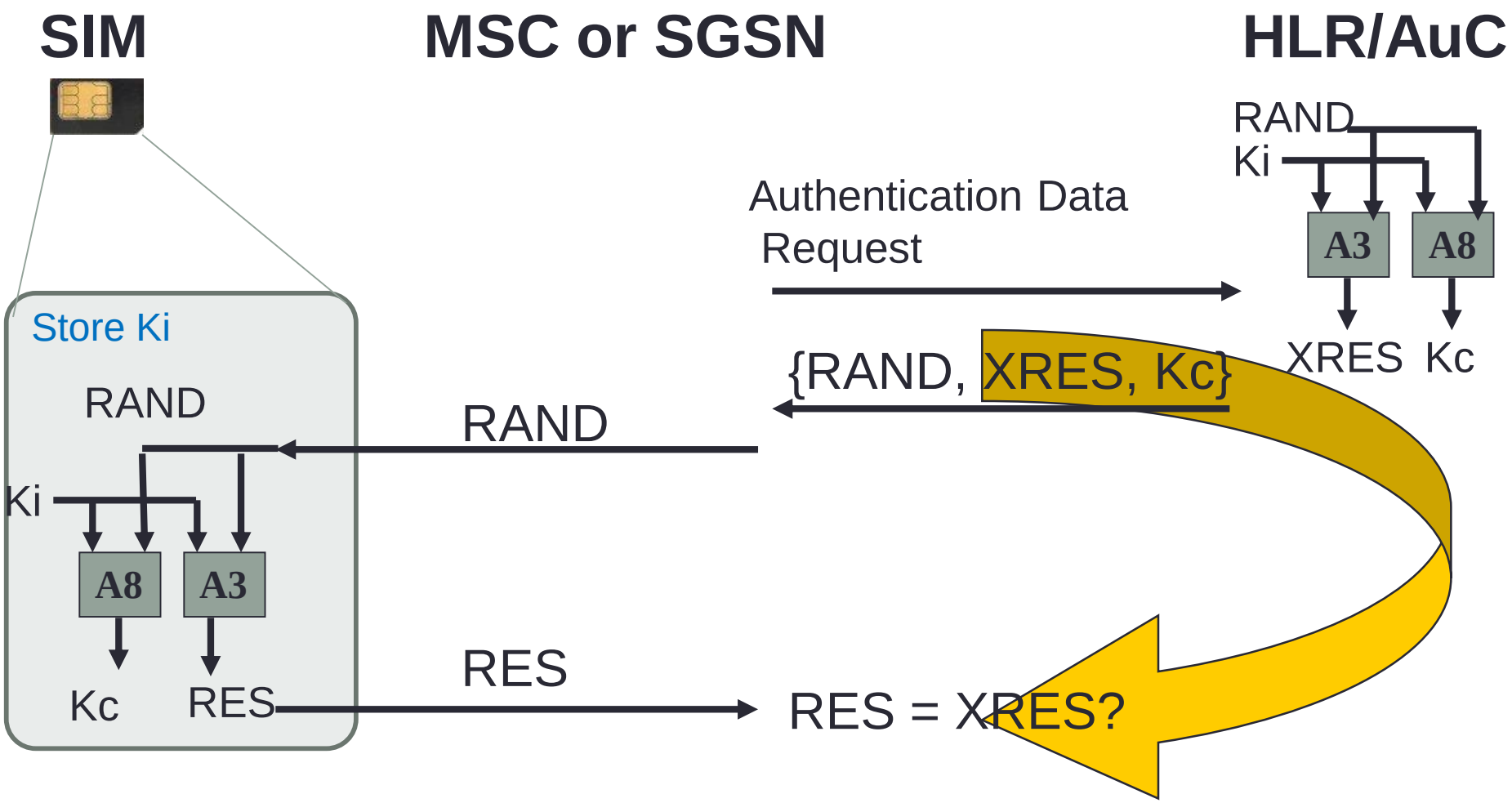
Part IV

- Threats
  - BOTNETS
  - (D)DOS

Part III

GSM AND LTE

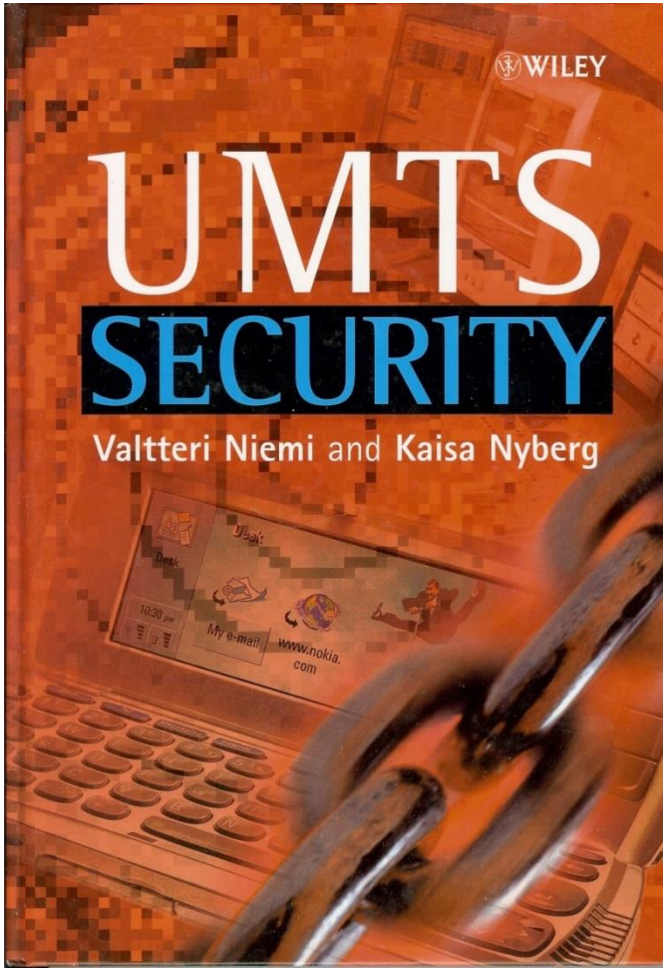
GSM Authentication and Key generation Protocol



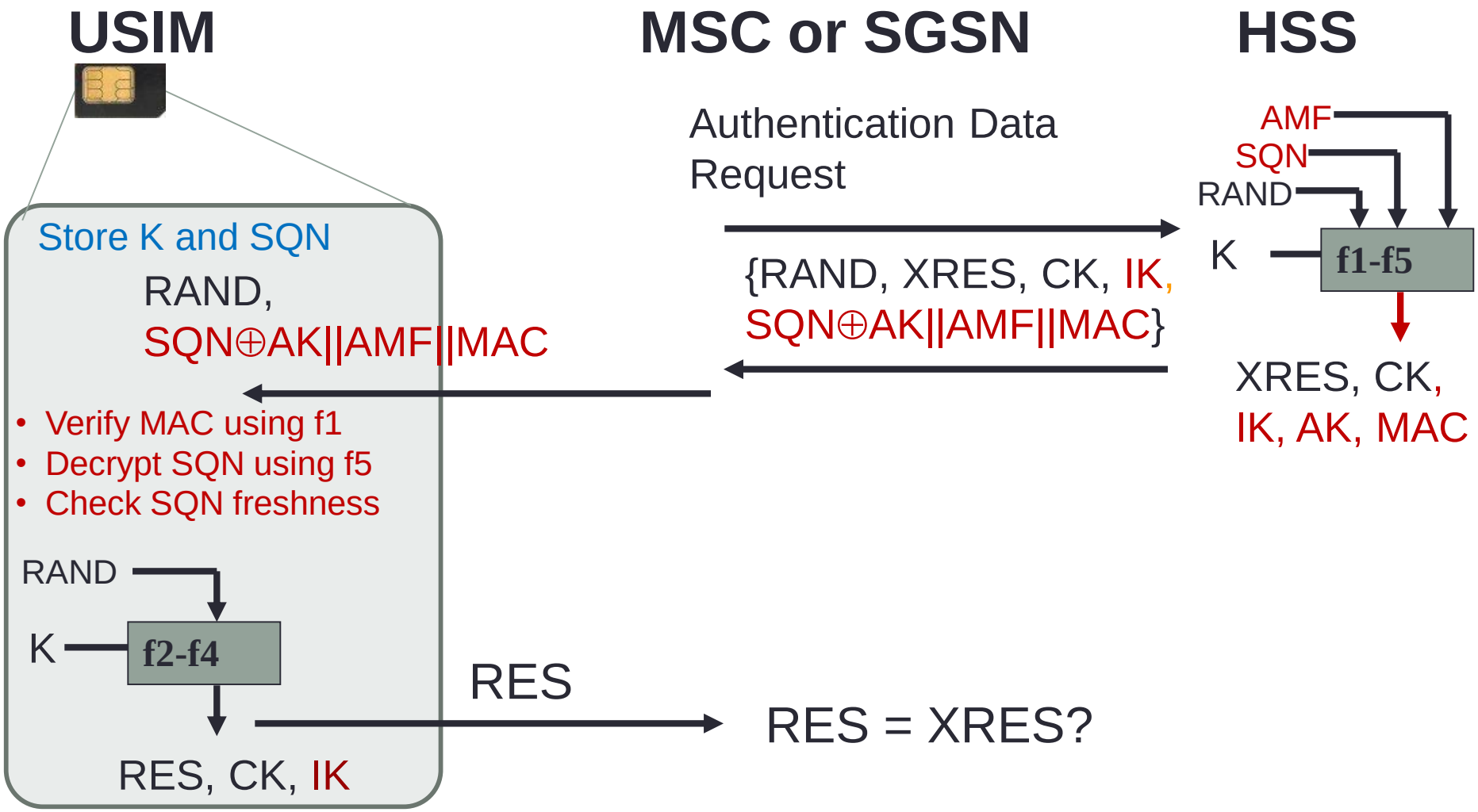
Recall the risk of a false base station attack

3G

- In 3G one introduced protection against false base stations
  - Mutual authentication (see next slide)
- Key length became 128 bit.



UMTS Authentication



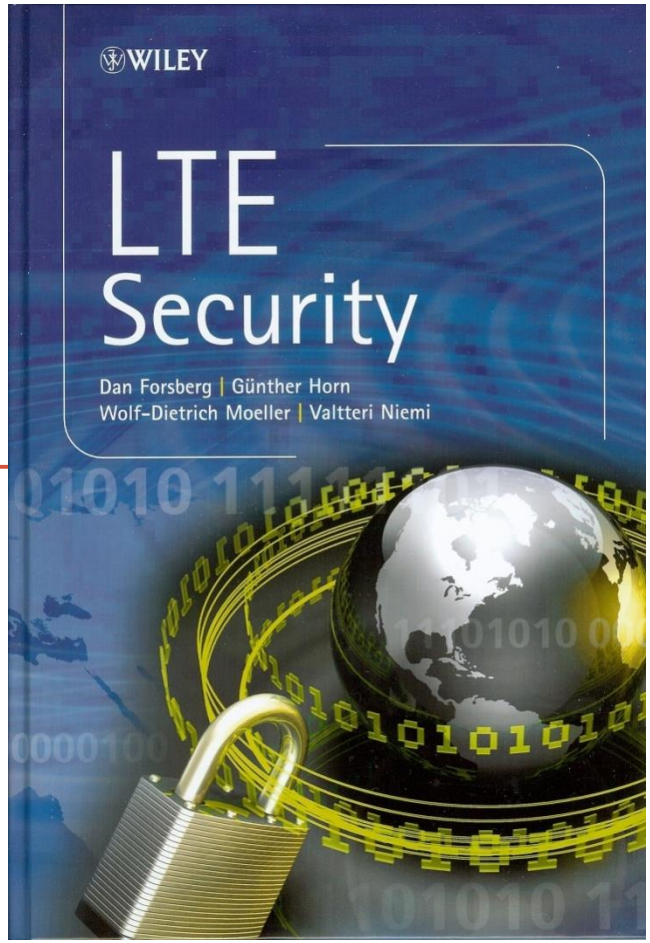
LTE SECURITY

GOALS:

Main concepts

Motivation

Differences with UMTS



LTE and EPS

- Long Term Evolution (LTE) is the mobile radio technology following after that of UMTS. The main motives to start the work on LTE were (again) increased capacity and throughput, and decreased latency.

- In parallel work was started on the Evolved Packet System (EPS) aiming for a simpler core network, and to integrate non-3GPP access technologies.

- For simplicity we only speak about LTE security

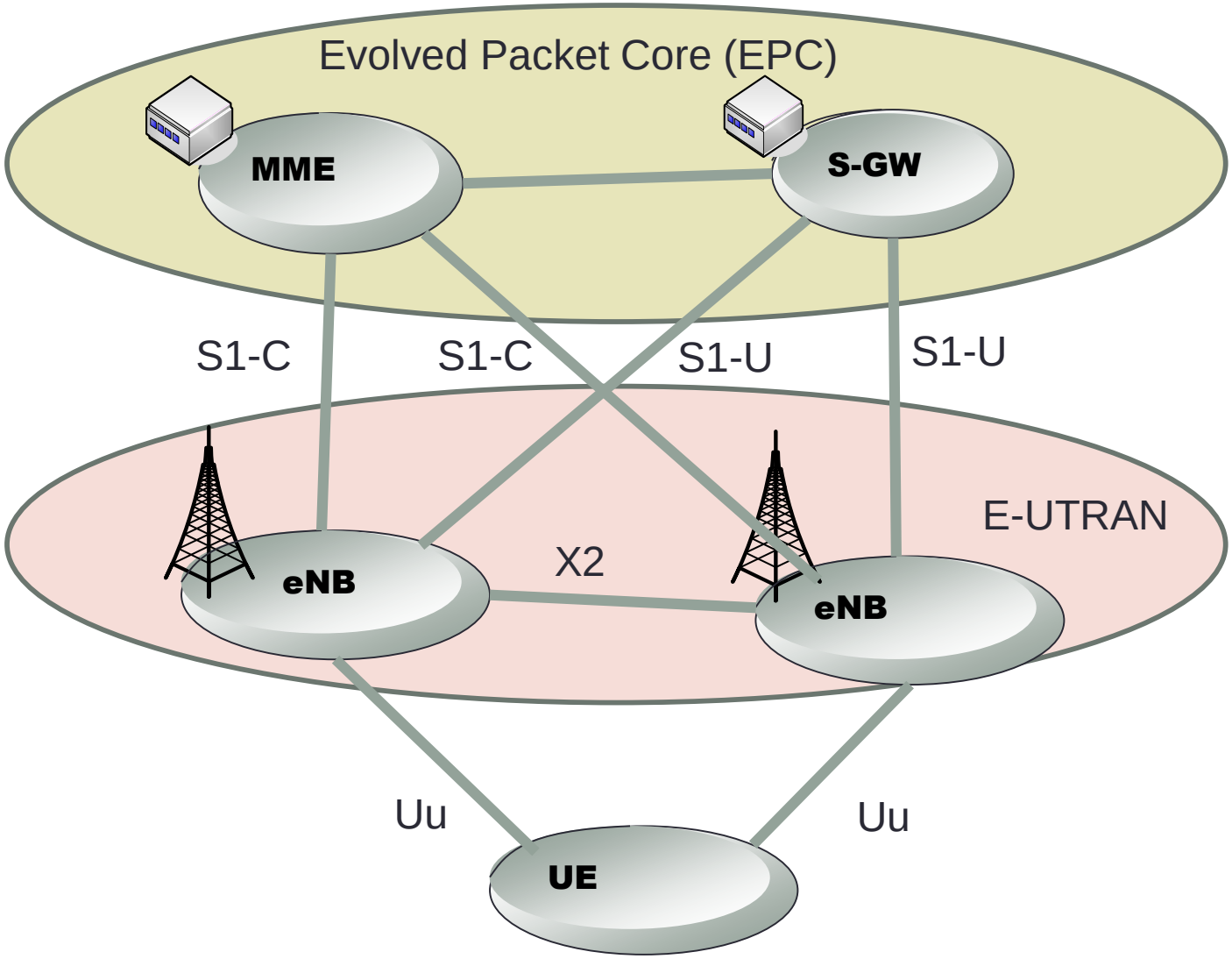
SAE / LTE terms

SAE = System Architecture Evolution
LTE = Long Term Evolution (of radio networks)

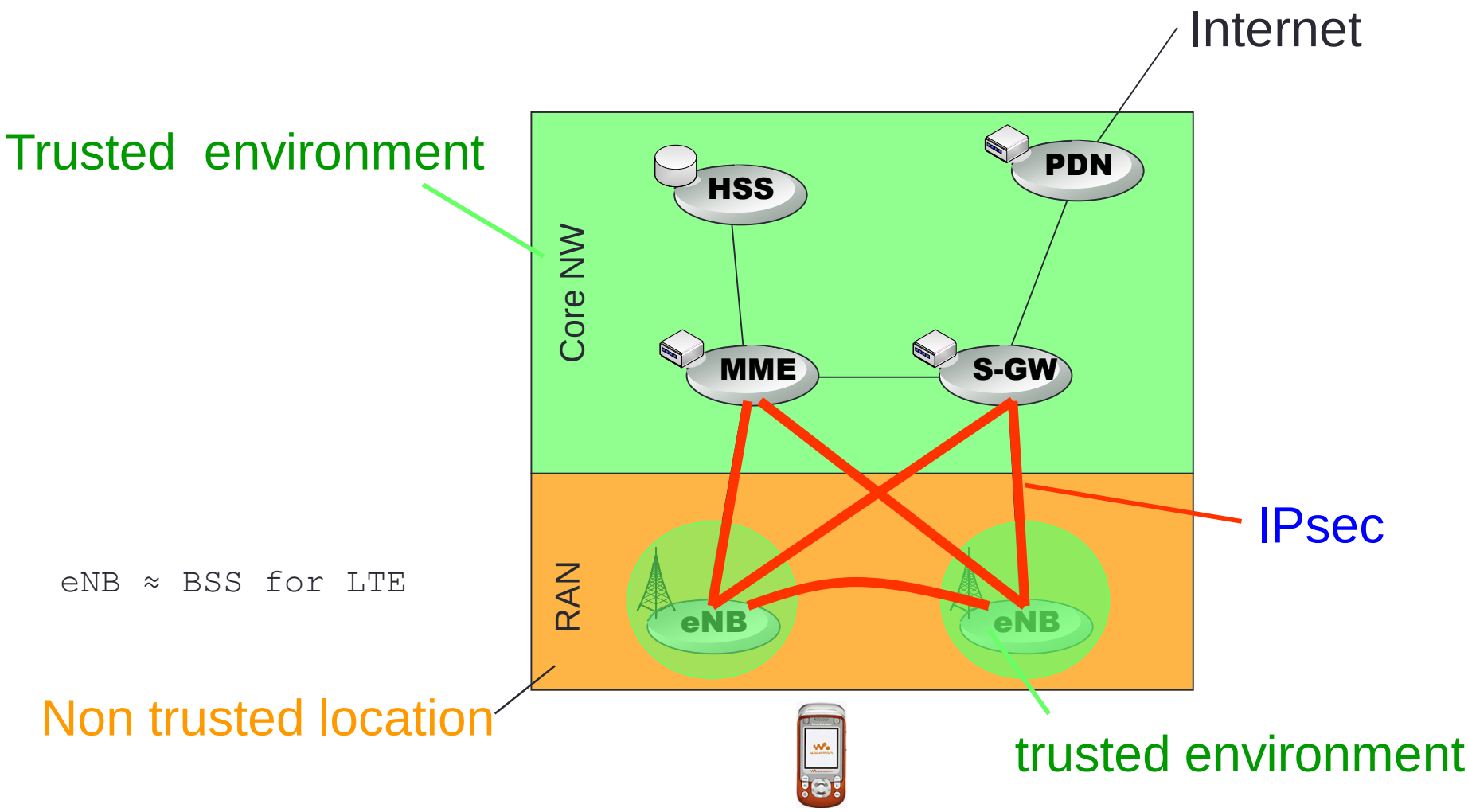
Technical terms:

- E-UTRAN = Evolved UTRAN (LTE radio network)
- EPC = Evolved Packet Core (SAE core network)
- EPS = Evolved Packet System (= RAN + EPC)
- MME= Mobility Management Entity
- eNB = base station
- UE = User Equipment (the user's modem)+…
- HSS = Home Subscriber Server
- PDN = packet data network
- SGW= Serving Gateway

Essential parts of EPS

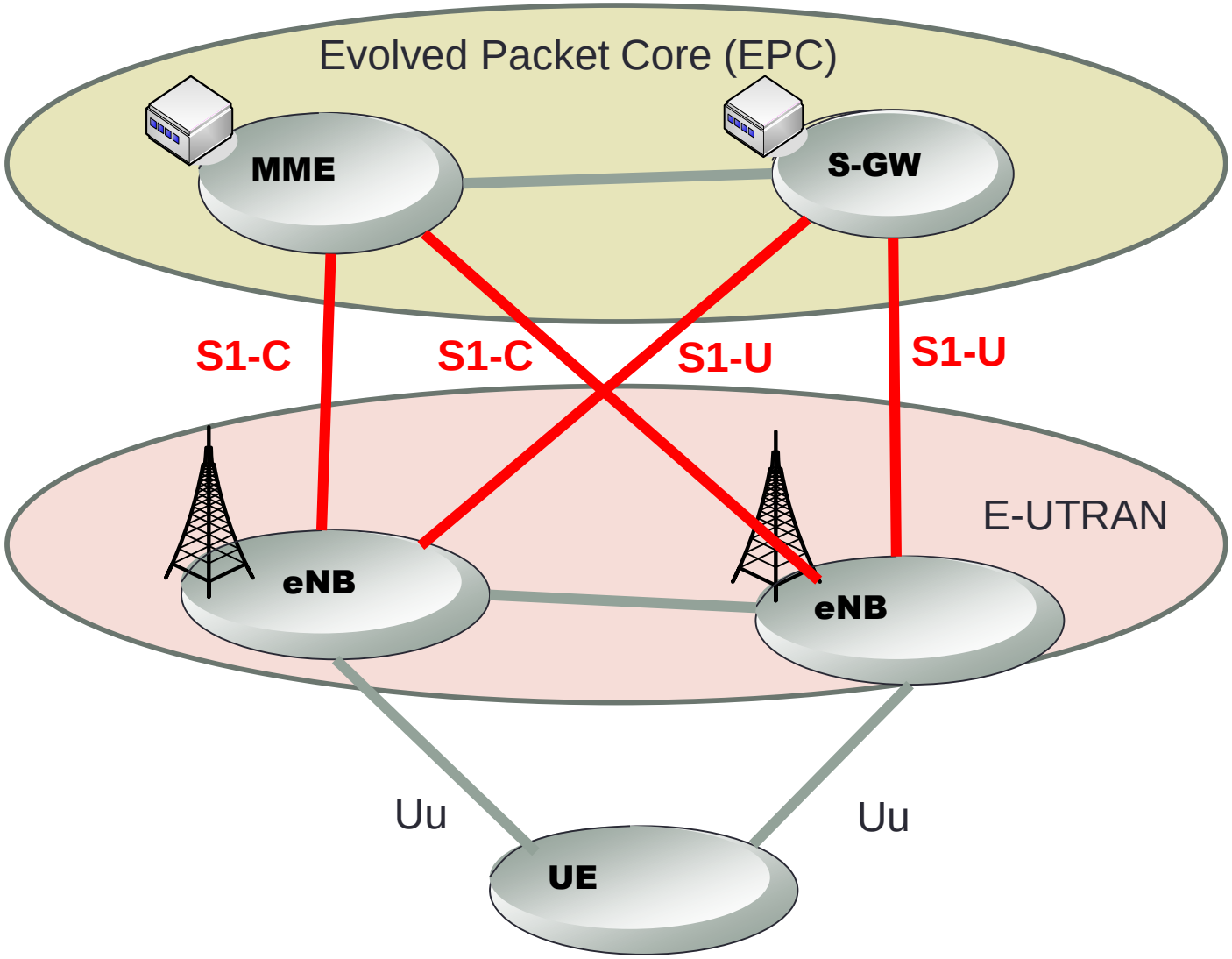


LTE Security architecture basics and trust assumptions

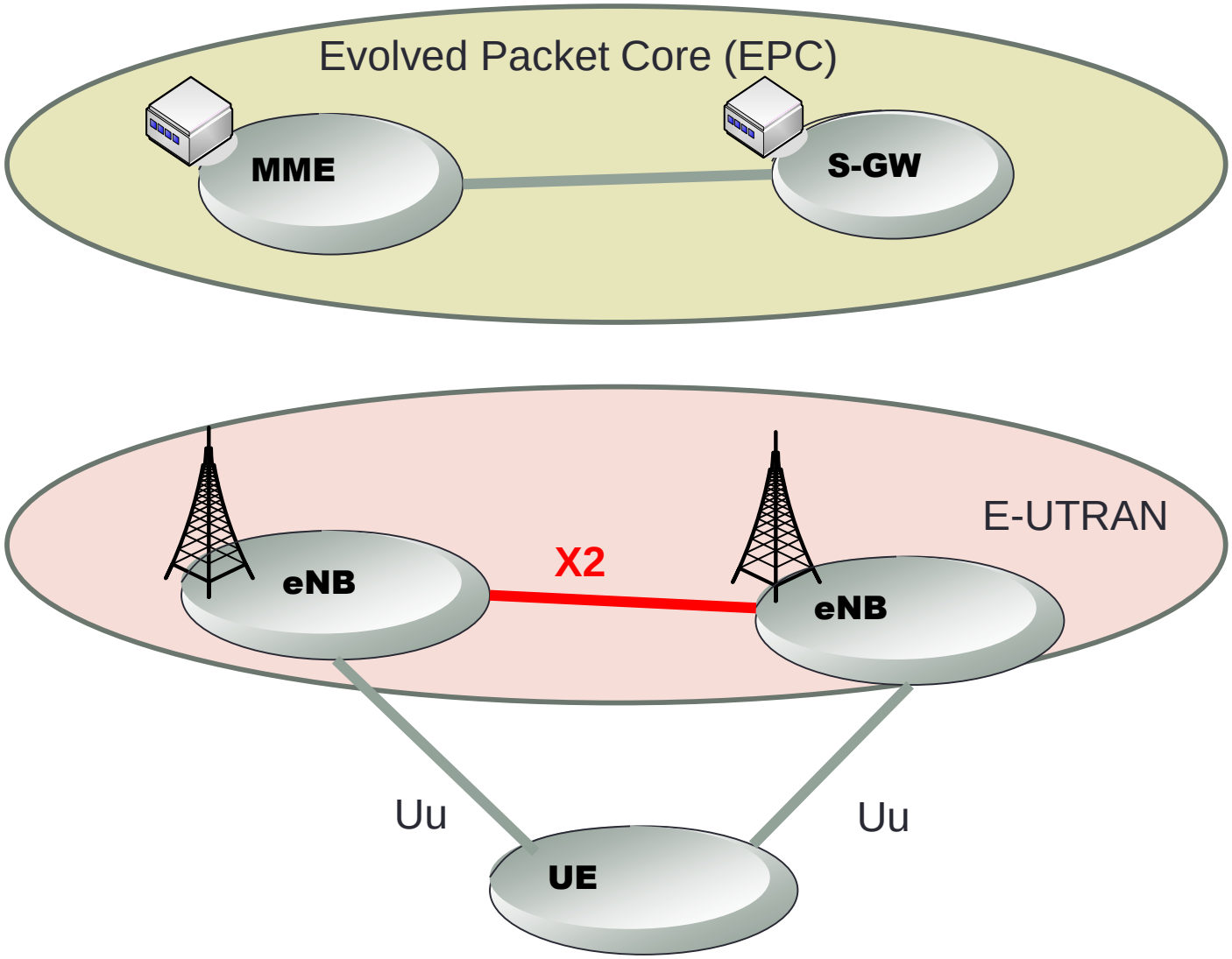


eNB ≈ BSS for LTE

S1 - handover


Evolved Packet Core (EPC)
MME
S-GW
S1-C
S1-C
S1-U
S1-U
E-UTRAN
eNB
eNB
Uu
Uu
UE

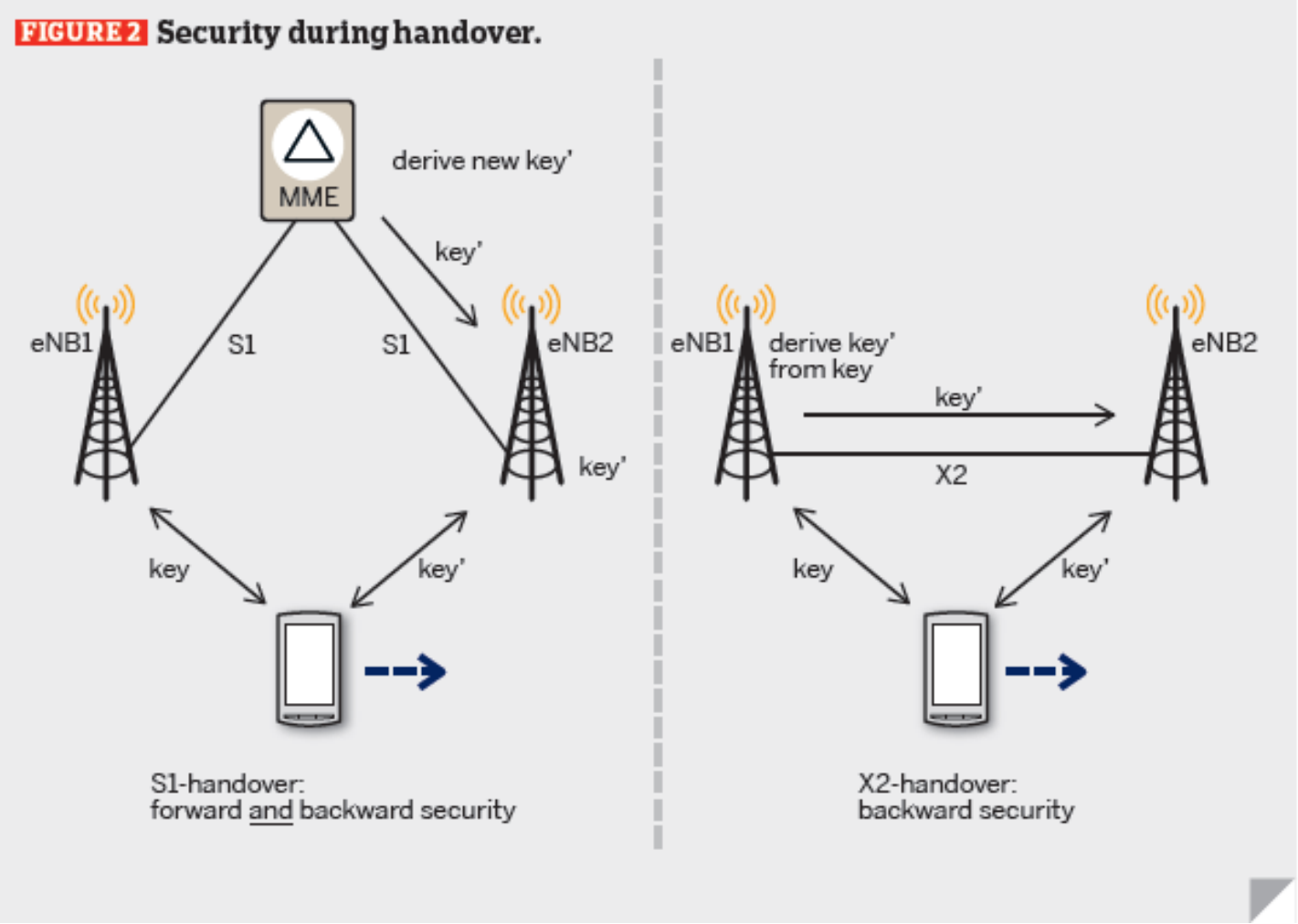
X2 handover



Mitigating the risk of false eNBs during handover

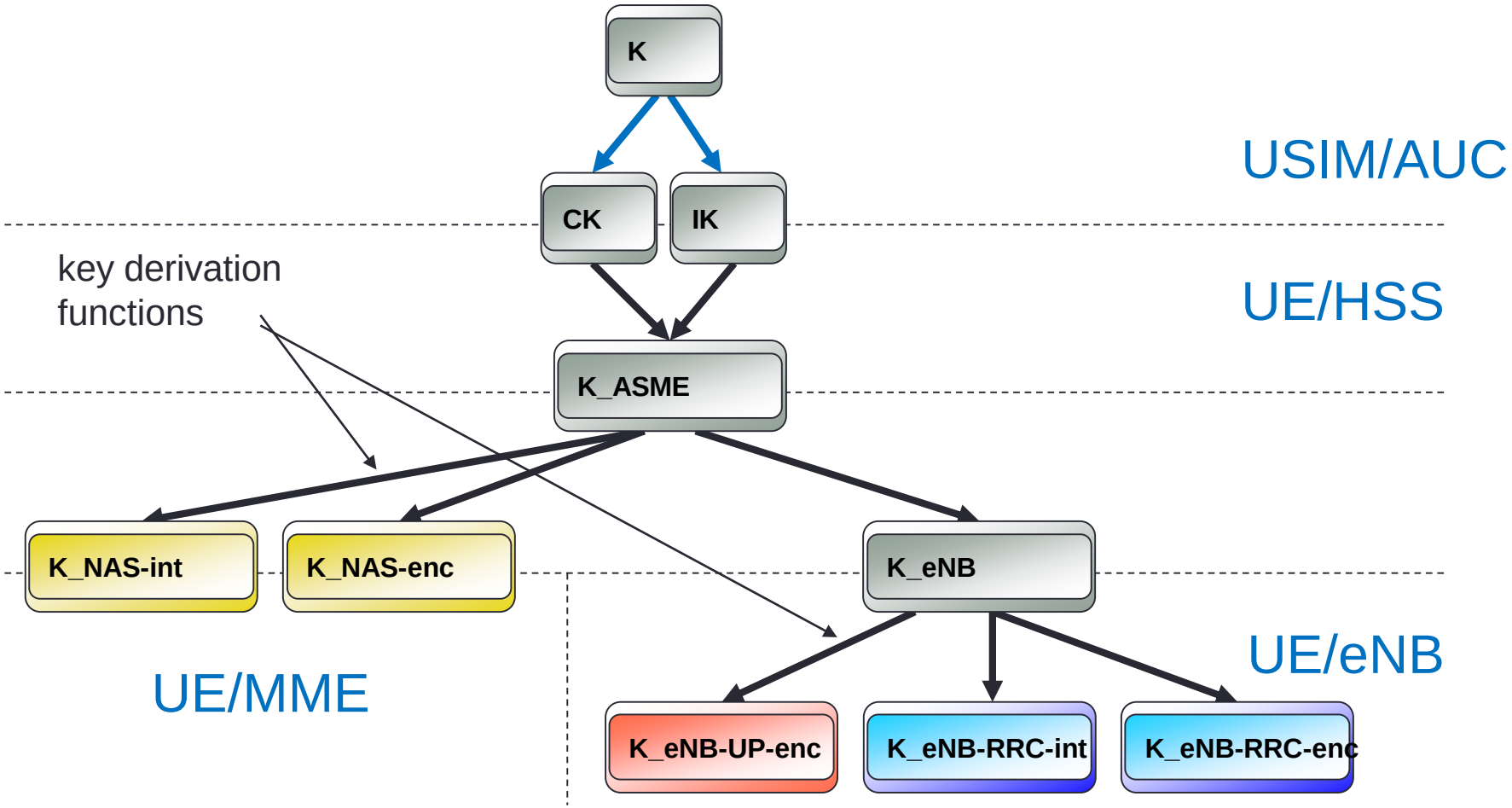
- When handover occurs between two eNBs, the source eNB needs to transfer security parameters to the target eNB
- Threats:
  - Source eNB is compromised
    - **Forward security**: recover from compromised source eNB
  - Target eNB is compromised
    - **Backward security**: keep previous traffic secure in case of compromised target eNB

Mitigating the risk of false eNBs during handover



Mandatory reading
Security in the Evolved Packet System R Blom, et all, 2010

LTE key hierarchy – different keys for different communication channels



Key Derivation Function (KDF)

- The KDF is the same as the KDF for the 3GPP Generic Bootstrap Architecture (GBA)
- It uses HMAC-SHA-256 and can thus generate a 256 bit result
- For KDF HMAC operates on a string S of the form
  - S = FC || P1 || L1 || P2 || L2 || … ||
  - Where || is concatenation operator and
    - FC = KDF usage depended octet
    - Pn is a data block of size Ln
    - Ln = two octet coding of length of Pn
- So Derived Key =KDF(K, S), K the key for the MAC

Example: KDF for K_ASME

- K=CK || IK
- S=
  - FC = 0x10,
  - P0 = SN id,
  - L0 = length of SN id (i.e. 0x00 0x03),
  - P1 = SQN ⊕ AK
  - L1 = length of SQN ⊕ AK (i.e. 0x00 0x06)
- K_ASME=KDF(K,S)
- More info see Appendix A in 3GPP TS 33.102

Device identity

- Note 1: The USIM is not the identity of the device but of the subscriber.
- Note 2: if the USIM is integrated into the device (in a non-removable manner) the USIM could act as the identity – in principle.
- Each mobile device has an identifier, the IMEI. However this is not a (strong) identity in the meaning of (secure) authentication.
  - IMEI can be cloned

The 3GPP standard requires the IMEI to be securely stored but that is still not enough to make it an identity.

LTE, GSM and IoT

- LTE has and will receive improvements to make it more attractive for IoT use but still the LTE radio is too expensive and power hungry for small battery operated IoT use cases that have to work a long time on one battery charge.
- For that reason NB-IoT has been developed as part of the LTE-Advanced Pro. As target cost $5 has been mentioned

- Many Machine-2-Machine use cases still use cheaper GSM technology which from security point of view is really bad.
  - Think about why is it bad?!

LTE Security - summary

- User plane security termination in eNB the main reason behind the elaborate key handling.
- Subscriber authentication almost exactly as in UMTS.
- The AKA procedure produces keys for a key hierarchy, in which keys are bound to their specific use;
- prepared for stronger 256-bit cryptography;
- a new key-updating mechanism for intra-LTE handovers;
- backhaul security;
- resistance to attacks on eNBs; and
- integration of security for non-3GPP accesses.
- Ciphering key depends on which algorithm is used for encryption (new feature in LTE)

Literature

Mandatory

- Security in the Evolved Packet System, R. Blom, et al. Ericsson Review, Oct 2010,

Background/additional

- 3GPP System Architecture Evolution (SAE), Security architecture, (Release 11), 3GPP TS 33.104
- UMTS Security, Valtteri Niemi and Kaisa Nyberg, Wiley, 2003
- LTE Security, D. Forsberg, et al, Wiley, 2010

Part III

INTERNET OF THINGS (IOT)

IoT module example; Mote

Development of a Mote for Wireless Image Sensor Networks
Ian Downes, Leili Baghaei Rad*, and Hamid Aghajan
Wireless Sensor Networks Laboratory, Department of Electrical Engineering
Stanford University, Stanford, CA 94305
Email: downes@stanford.edu, leili@ieee.org, aghajan@stanford.edu

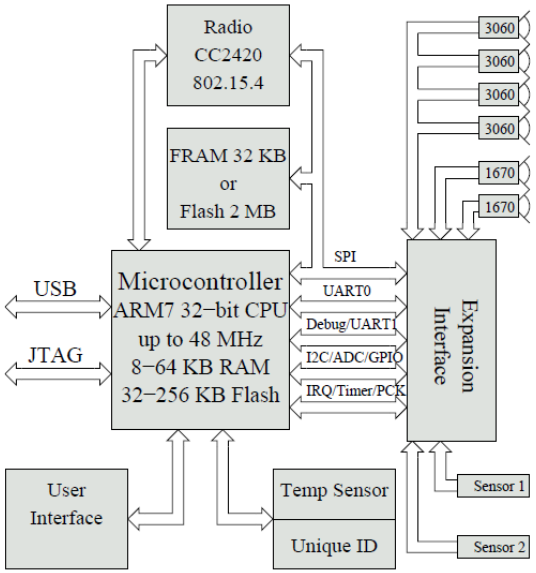
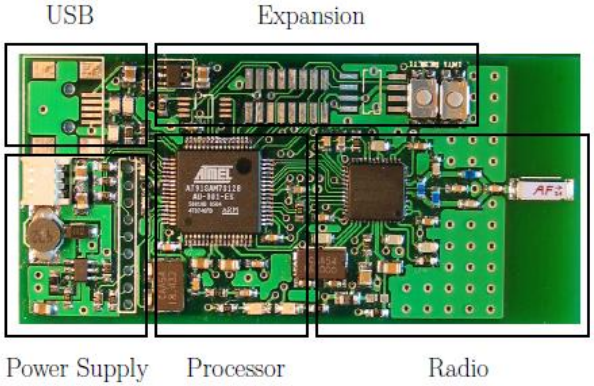
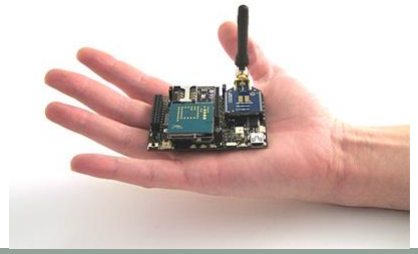


Fig. 5. System diagram of the mote board.



Wasp Mote



Security aspects

- Efficient protocols for IoT
  - Energy efficient foremost
  - Easy to deploy and to manage becomes of the large numbers
- Bootstrapping of security
  - How to arrange a secure setup: credentials and configurations
- Life-cycle management
  - Bootstrapping problem
  - SW updates
  - Repair flow (if any, maybe to expensive to repair wrt cost of device)
  - End-of-life handling.

Wireless sensor nodes

- Energy needed for transmission is often the dominating part of the total energy needed to operate a sensor node*)
  - So even complex crypto is often not a problem
  - ECC is nice because it keeps the number of bits down

- *) one bit shift operation: 0,08pJ

  one bit transmission: 20nJ

So sending a bit takes 250 000 times more energy than ”computing” a bit

Source: A Survey of Wireless Mesh Networking Security Technology and Threats, SANS Report

Part IV

MALWARE IN THE (INTER)NET

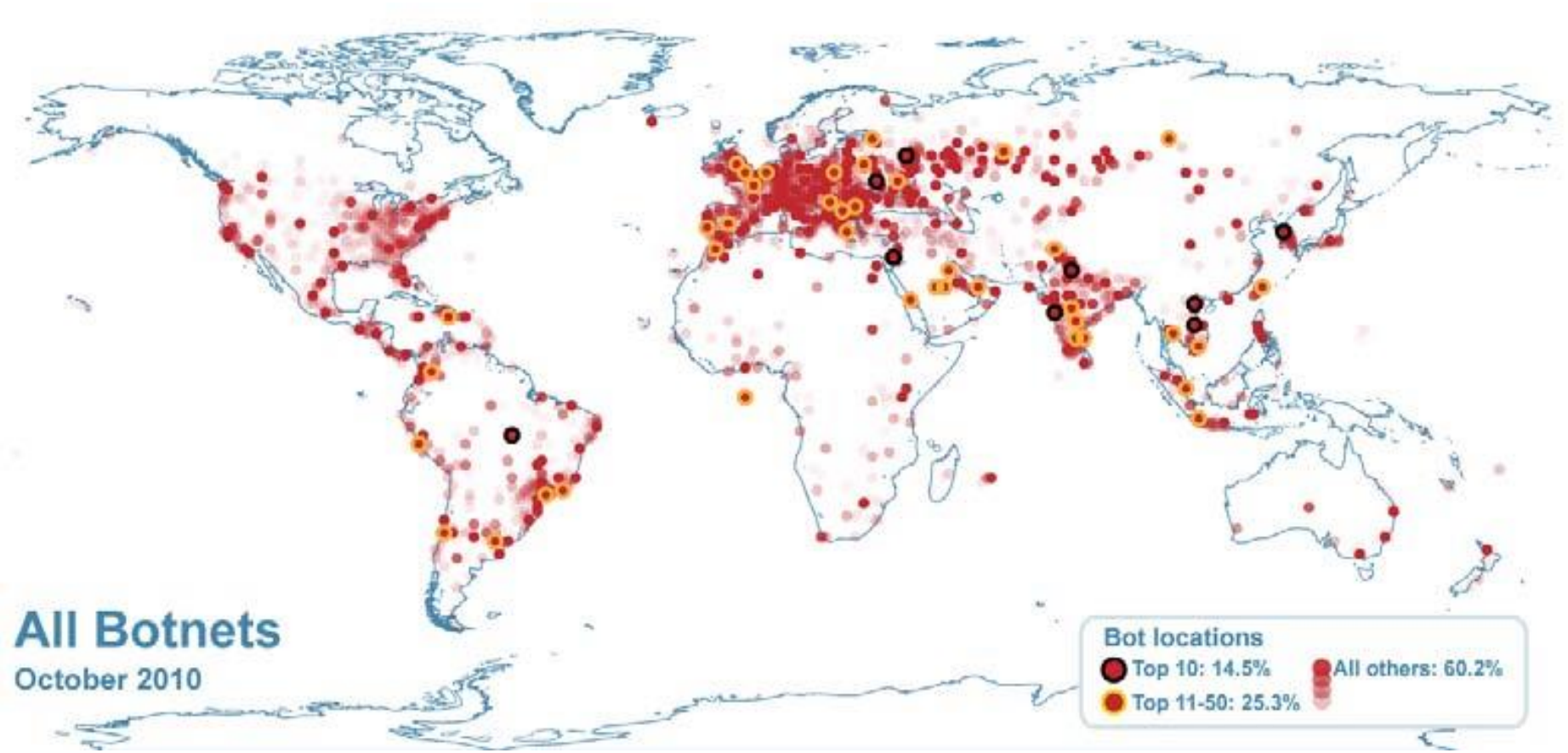
Bad things in the network

- A lot ….

We talk here about

- Botnet nets
- Attacking infrastructure
  - Denial of Service Attacks
  - Attacking network (processing) nodes -> for later

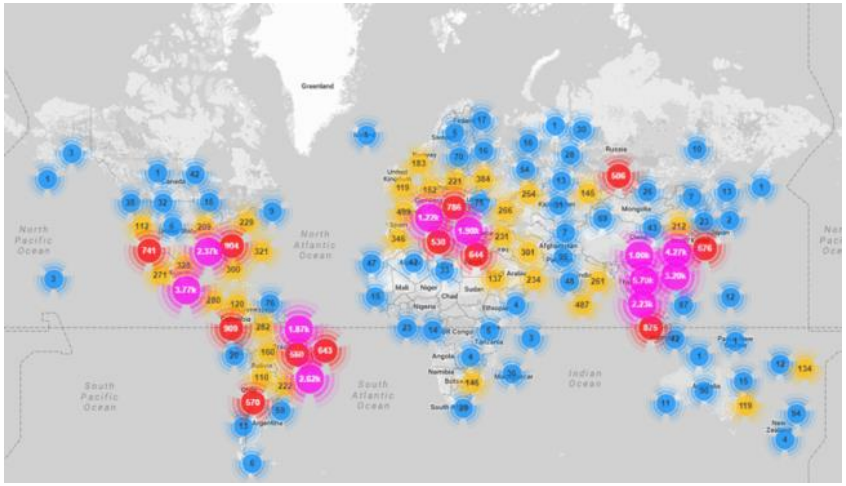
Where are botnets?



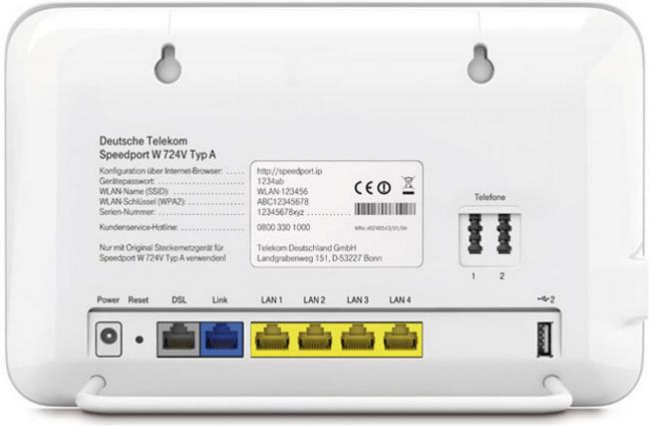
Source, Symantec 2010

Mirai and Mirai variants

The Mirai botnet appeared in August 2016 and has been used in some of the largest and most disruptive distributed denial of service (DDoS) attacks using Internet of things (IoT) devices, IP cameras and routers

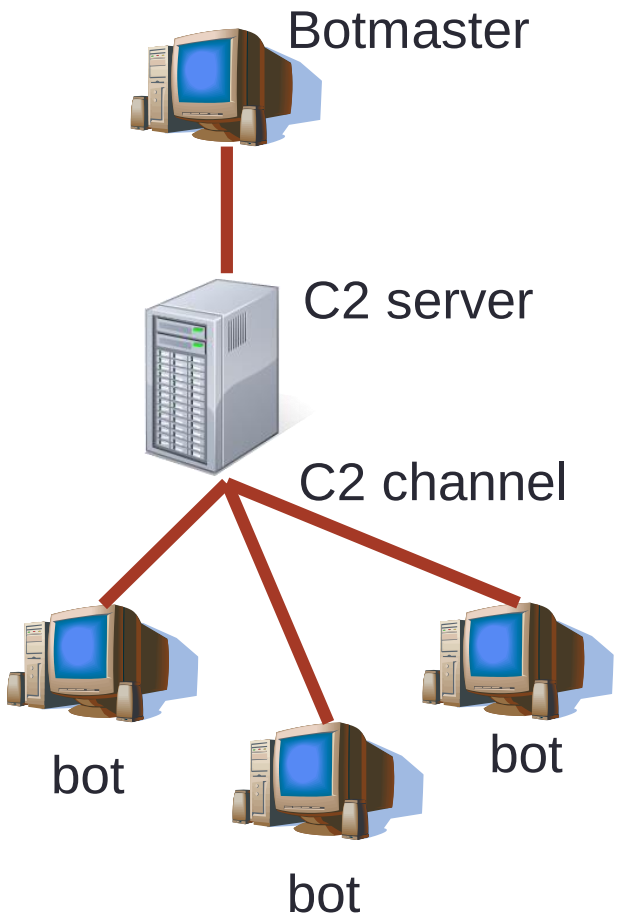


November 2016, 900,000 customers of German ISP Deutsche Telekom got their routers attacked to form a botnet



Botnet architecture

- Bots: malicious, self-propagated program
- Command and Control (C2) servers:
  - intermediate through which the botmaster control botnet
  - usually are “bullet-proof" servers
- Command and Control channel: communication protocol between bots and C2 servers (e.g. IRC, HTTP, P2P)
- Proxies (optional):
  - Redirect trac between C2 servers and bot in order to hide identities of C2 servers
  - Usually selected among bots with public accessibility and high bandwidth



Challenge for botnets

- C2 servers and channel are weakest links of botnets and most detection and botnet mitigation techniques aim for breaking their operation.

- Botnet therefor deploy evasion mechanims to:
  - Disguise communication channel: encrypted IRC, HTTP, social network
  - Hide the identity of C2 servers: hard-coded IP list, distributed DNS, proxies...
    - DNS evasive techniques – DNS entries should not (easily) reveal where the attacker is

Examples of DNS evasive techniques

- Fast flux
- Domain flux

RECALL: A and NS records

foo.com.	NS	ns1.bar.com.
foo.com.	A	192.168.100.1

Fast (or IP)-flux

- The main idea behind Fast flux is to have many IP addresses associated with a single fully qualified domain name, where the IP addresses are swapped in and out with extremely high frequency, through changing DNS records. Hence multiple IPs map to one domain: set A or NS records
  - Change rapidly: low TTL value (as often as 3 mins.)
  - Double-flux not only fluxes the IP addresses associated with the FQDN, but also fluxes the IP addresses of the DNS servers (e.g., A records) that are in turn used to lookup the IP addresses of the FQDN

Time-to-live (TTL) is a value in an Internet Protocol (IP) packet that tells a network router whether or not the packet has been in the network too long and should be discarded. In IPv6 the TTL field in each packet has been renamed the hop limit.

- Typical use:
  - illegal contents hosting, malicious software distribution...
  - Examples: Storm Worm, TDL4...

Domain Flux

- Domain flux is effectively the inverse of IP flux and refers to the constant changing and allocation of multiple FQDN's to a single IP address or C2 infrastructure.
- Domain names are generated by a Domain Generation Algorithm (DGA) (hundreds to thousands)
  - Botmaster registers one of the domain in the list
  - I Bot tries each domain in the list until it is resolvable
- Typical use:
  - Exhausting blacklisting effort
  - Examples: Concker, Torpig, Kraken...

;;Kraken bot DGA
rbqdxflojkj.mooo.com
bltjhzqp.dyndns.org
cffxugijxn.yi.org
etllejr.dynserv.com
ejfjyd.mooo.com
mnkzof.dyndns.org
adhbtib.yi.org
vqsqul.dynserv.com
dawjjopw.mooo.com
jamptmlvrw.dyndns.org
ihouxyds.yi.org
fvkvwf.dynserv.com
duxhvrrb.mooo.com
natiouwx.dyndns.org
afmbtgyktty.yi.org
eltxytxurng.dynserv.com
tmuncana.mooo.com
wafyfrryfzr.dyndns.org
lbimniu.yi.org
fqjhsvsevdy.dynserv.com
zstyderw.mooo.com
ouwyrav.dyndns.org
utndjeqx.yi.org
Linh

Botnet literature

Mandatory reading

- Understanding the Mirai Botnet, M Antonakakis, et all, Usenix, Aug. 2017.

Background reading

- D. Dagon, G. Gu, C. Lee, and W. Lee, A taxonomy of botnet structures," Computer Security Applications Conference, Annual, vol. 0, pp. 325-339, 2007.
- MessageLabs, MessageLabs Intelligence: 2010 Annual Security Report," 2010. [Online Available]: http://www.symanteccloud.com/mlireport/MessageLabsIntelligence 2010 Annual Report FINAL.pdf
- DDOS evolution: http://187.7.106.14/wiki2015_1/lib/exe/fetch.php?media=ddos.pdf

Denial-of-Service Attacks

- DOS attacks **distributed DOS (DDOS)** aim at making a service unavailable to its intended users.

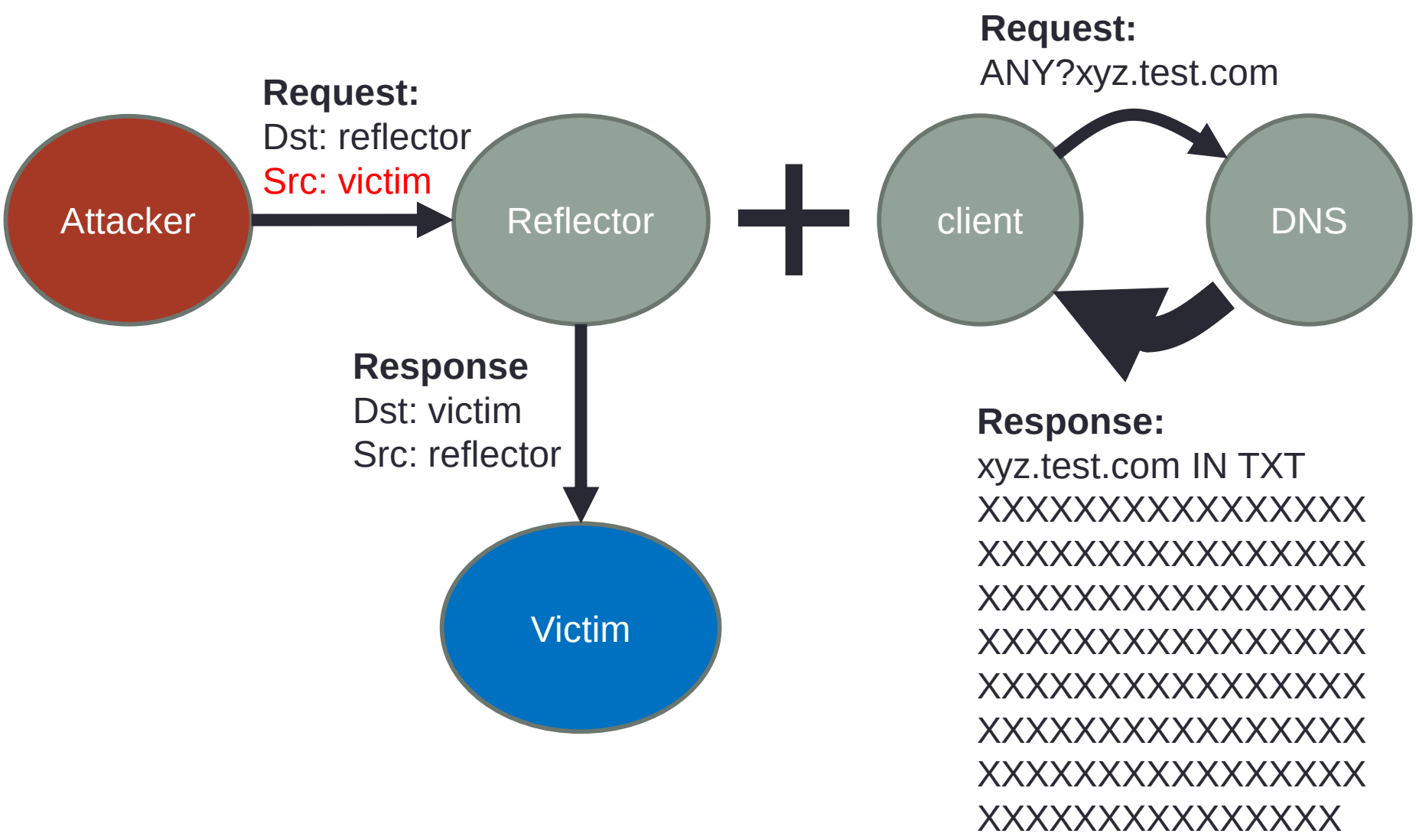
- Normally done by remotely attacking the server(s) that provide the service

Origin of DOS attacks

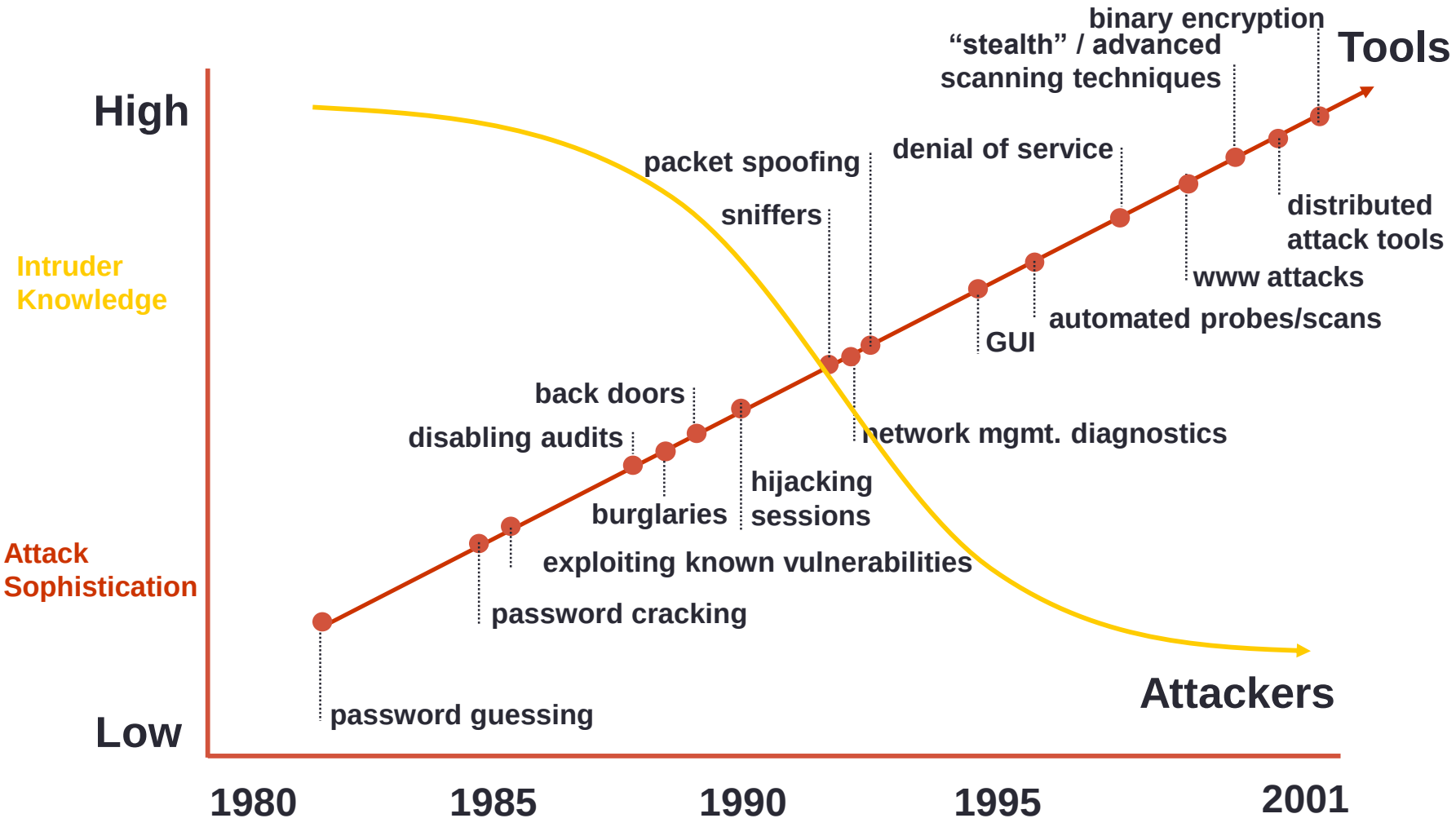
(D)DOS attacks are possible because of

- Errors in the protocol stack, e.g. ping-of-death, reflection
- Network setup errors
- Resource constraints (mostly this type)

DNS Amplification attack= reflection + amplification



DDOS attack tools evolution



Countermeasures against DDOS

Use a combination of different approaches:

1. Mitigate and detect.

2. Analytics; distinguish as good as possible good traffic from bad traffic to preserve business continuity,

3. Planning of resources:
   - include performance and architecture to deploy upstream to protect all points of vulnerability.
   - Maintain reliable and cost-efficient scalability.

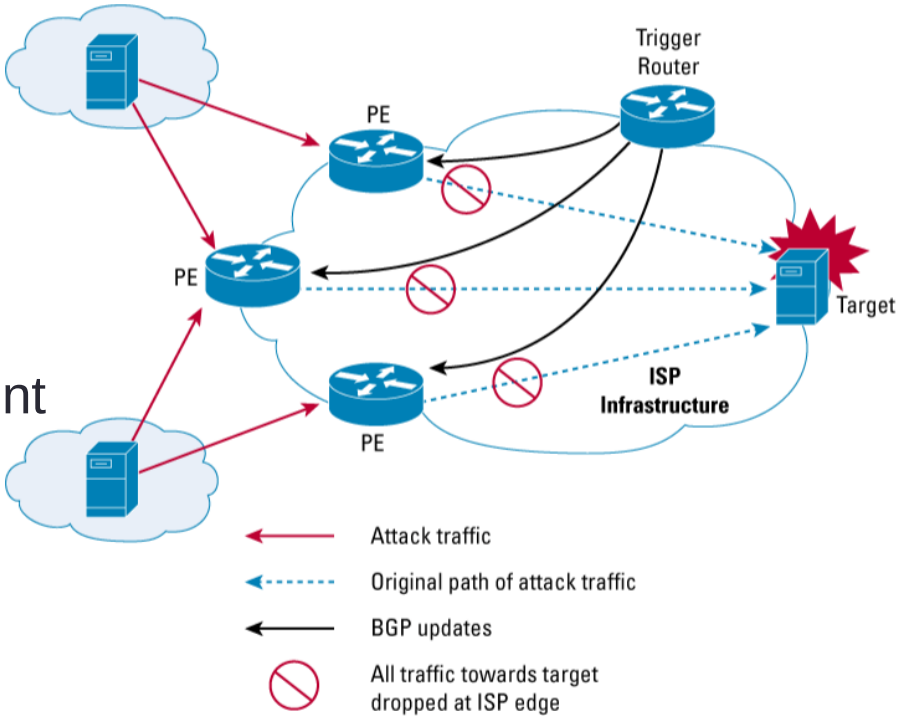
Countermeasures against DDOS

- No 100% solution exist today
- Filtering techniques
  - Source checking techniques
  - Rate-limiting techniques
  - Blackhole routing
- Organisational
  - Regular review of systems capacity
  - Dynamic rerouting/load balacing
  - Network surveillance
  - Blackhaul routing

Blackhole routing

- Different approaches
  - See Cisco blackhole http://www.cisco.com/web/about/security/intelligence/blackhole.pdf
  - Software Defined Networks (SDN) – allows flexibility in resource use and deployment

Figure 1. Destination-Based Black Hole Filtering with Remote Triggering



Cisco:

DDOS and DNSSEC

- Secure DNS, DNSSEC, has been introduced to mitigate security problems with DNS functionality.

- However, it can be a vehicle for DDOS attacks as DNSEC can induce demanding processing.

- See **background reading**:
- DNSSEC and Its Potential for DDoS Attacks, R v Rijswijk-Deij, A Sperotto, A, Pras, IMC'14, November 5–7, 2014, Vancouver, BC, Canada.