Security and Privacy in Upcoming Wireless Networks

Security and Privacy in Upcoming Wireless Networks

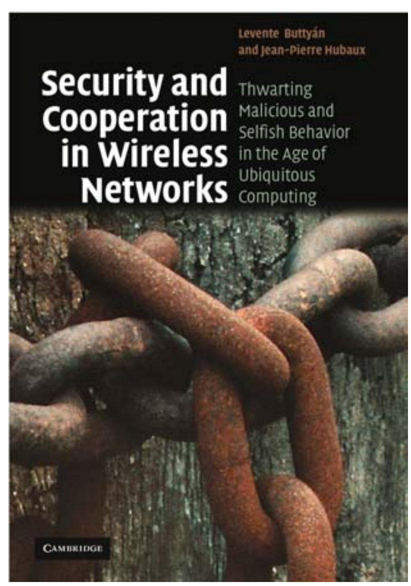
Lectures presented at

SWING'07, Bertinoro, Italy, 2007

by Levente Buttyán

A textbook

- written by
  - Levente Buttyan (BME)
  - Jean-Pierre Hubaux (EPFL)
- intended to
  - graduate students
  - researchers and practitioners
- to be published by
  - Cambridge University Press
  - ISBN 9780521873710
- expected publication date
  - November 2007
- material available on-line at **secowinet.epfl.ch**
  - full manuscript in pdf
  - slides for each chapter (progressively)



Program

Day 1	– Classical introduction to security and cryptography – Upcoming wireless networks and new challenges for security and privacy
Day 2	– Secure routing in ad hoc and sensor networks
Day 3	– Provable security for routing protocols – Wormhole detection techniques
Day 4	– Attacks on addressing (and some solutions) – Key establishment in ad hoc and sensor networks
Day 5	– Symmetric-key private authentication (in RFID systems) – Location privacy in vehicular networks

Security and Privacy in Upcoming Wireless Networks

Classical introduction to security and cryptography

symmetric and asymmetric key encryption;
hash functions;
MAC functions;
digital signatures;
key establishment protocols;

Security

- security is about how to prevent attacks, or – if prevention is not possible – how to detect attacks and recover from them
- an attack is a a *deliberate attempt* to compromise a system; it usually exploits weaknesses in the system's design, implementation, operation, or management
- attacks can be
  - passive
    - attempts to learn or make use of information from the system but does not affect system resources
    - examples: eavesdropping message contents, traffic analysis
    - difficult to detect, should be prevented
  - active
    - attempts to alter system resources or affect their operation
    - examples: masquerade (spoofing), replay, modification (substitution, insertion, destruction), denial of service
    - difficult to prevent, should be detected

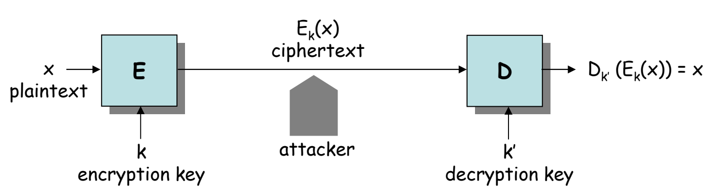
Main security services

- authentication
  - aims to detect masquerade
  - provides assurance that a communicating entity is the one that it claims to be
- access control
  - aims to prevent unauthorized access to resources (information, services, and devices)
- confidentiality
  - aims to protect data from unauthorized disclosure
  - usually based on encryption
- integrity
  - aims to detect modification and replay of messages
  - provides assurance that data received are exactly as sent by the sender
- non-repudiation
  - provides protection against denial by one entity involved in a communication of having participated in the communication
  - two basic types: non-repudiation of origin and non-repudiation of delivery

Some security mechanisms

- encryption
  - symmetric key, asymmetric (public) key
- digital signature
- access control schemes
  - access control lists, capabilities, security labels, ...
- data integrity mechanisms
  - message authentication codes, sequence numbering, time stamping, cryptographic chaining
- authentication protocols
  - passwords, cryptographic challenge-response protocols, biometrics
- traffic padding, routing control, …

Operational model of encryption



- attacker's goal:
  - to systematically recover plaintext from ciphertext
  - to deduce the (decryption) key
- Kerckhoff's assumption:
  - attacker knows all details of E and D
  - attacker doesn't know the (decryption) key

Attack models

- ciphertext-only attack
  - the adversary can only observe ciphertexts produced by the same encryption key
- known-plaintext attack
  - the adversary can obtain corresponding plaintext-ciphertext pairs produced with the same encryption key
- (adaptive) chosen-plaintext attack
  - the adversary can choose plaintexts and obtain the corresponding ciphertexts
- (adaptive) chosen-ciphertext attack
  - the adversary can choose ciphertexts and obtain the corresponding plaintexts
- related-key attack
  - the adversary can obtain ciphertexts, or plaintext-ciphertext pairs that are produced with different encryption keys that are related in a known way to a specific encryption key

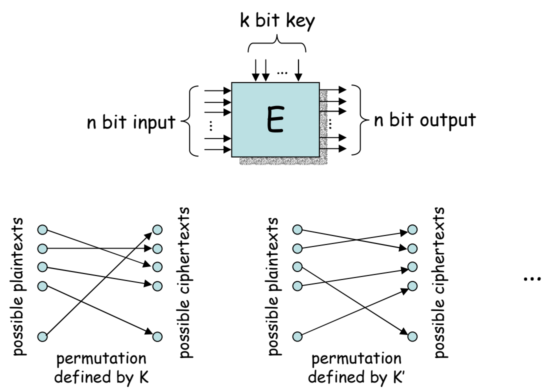
Basic classification of encryption schemes

- symmetric-key encryption
  - it is easy to compute K' from K (and vice versa)
  - usually K' = K
  - two main types:
    - stream ciphers – operate on individual characters of the plaintext
    - block ciphers – process the plaintext in larger blocks of characters
- asymmetric-key encryption
  - it is hard (computationally infeasible) to compute K' from K
  - K can be made public (→ public-key cryptography)

Block ciphers

an *n* bit block cipher is a function E: $\{0, 1\}^n \times \{0, 1\}^k \rightarrow \{0, 1\}^n$, such that for each $K \in \{0, 1\}^k$, $E(., K) = E_K : \{0, 1\}^n \rightarrow \{0, 1\}^n$ is a **strong pseudorandom permutation**

(i.e., practically indistinguishable from a randomly chosen permutation even if the adversary is given oracle access to the inverse of the permutation)

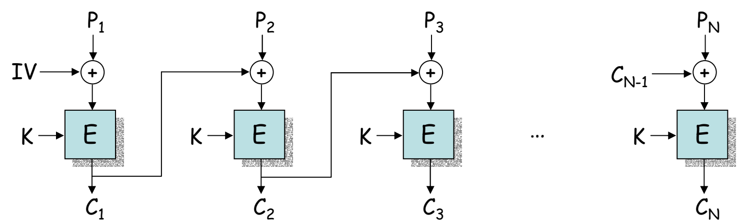


Block cipher modes of operation

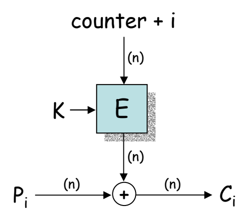
- ECB – Electronic Codebook
  - used to encipher a single plaintext block (e.g., a DES key)
- CBC – Cipher Block Chaining
  - repeated use of the encryption algorithm to encipher a message consisting of many blocks
- CFB – Cipher Feedback
  - used to encipher a stream of characters, dealing with each character as it comes
- OFB – Output Feedback
  - another method of stream encryption, used on noisy channels
- CTR – Counter
  - simplified OFB with certain advantages

Frequently used modes

- CBC



- CTR



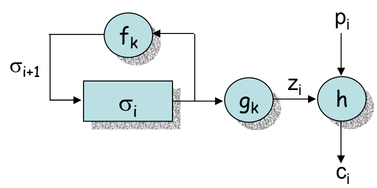
Stream ciphers

- while block ciphers simultaneously encrypt groups of characters, stream ciphers encrypt individual characters
  - may be better suited for real time applications
- stream ciphers are usually faster than block ciphers in hardware (but not necessarily in software)
- limited or no error propagation
  - may be advantageous when transmission errors are probable

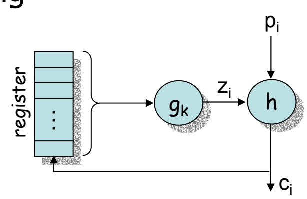
- note: the distinction between stream ciphers and block ciphers is not definitive
  - stream ciphers can be built out of block ciphers using CFB, OFB, or CTR modes
  - a block cipher in ECB or CBC mode can be viewed as a stream cipher that operates on large characters

Types of stream ciphers

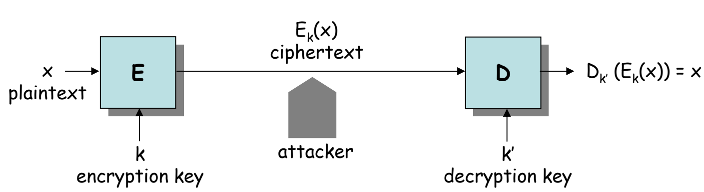
- synchronous



- self-synchronizing

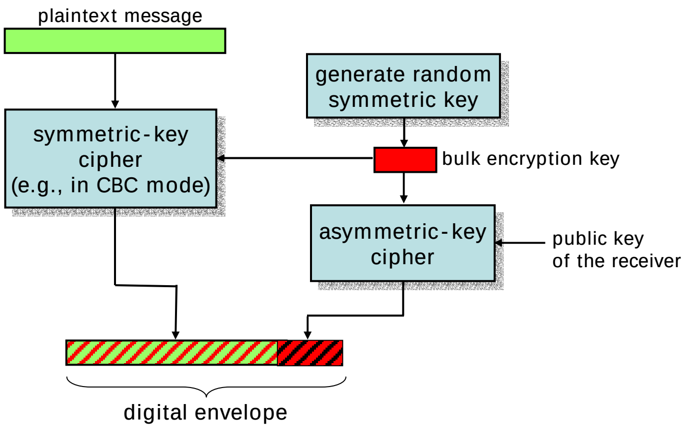


Public-key cryptography



- asymmetric-key encryption
  - it is hard (computationally infeasible) to compute k' from k
  - k can be made public (public-key cryptography)
- public-keys are not confidential but they must be authentic !
- most popular public-key encryption methods (e.g., RSA) are several orders of magnitude slower than the best known symmetric key schemes

Hybrid encryption (digital envelope)

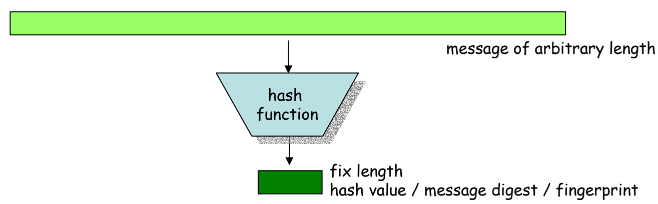


Examples for hard problems

- factoring problem
  - given a positive integer n, find its prime factors
    - true complexity is unknown
    - it is believed that it does not belong to P
- discrete logarithm problem
  - given a prime p, a generator g of Z_p^*, and an element y in Z_p^*, find the integer x, $0 \leq x \leq p-2$, such that $g^x \bmod p = y$
    - true complexity is unknown
    - it is believed that it does not belong to P
- Diffie-Hellman problem
  - given a prime p, a generator g of Z_p^*, and elements $g^x \bmod p$ and $g^y \bmod p$, find $g^{xy} \bmod p$
    - true complexity is unknown
    - it is believed that it does not belong to P

Hash functions

- a hash function maps bit strings of arbitrary finite length to bit strings of fixed length (n bits)
- many-to-one mapping → collisions are unavoidable
- however, finding collisions are difficult → the hash value of a message can serve as a compact representative image of the message (similar to fingerprints)

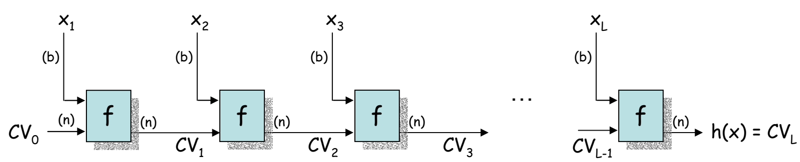


Desirable properties of hash functions

- ease of computation
  - given an input x, the hash value h(x) of x is easy to compute
- weak collision resistance (2nd preimage resistance)
  - given an input x, it is computationally infeasible to find a second input x′ such that h(x′) = h(x)
- strong collision resistance (collision resistance)
  - it is computationally infeasible to find any two distinct inputs x and x′ such that h(x) = h(x′)
- one-way hash function (preimage resistance)
  - given a hash value y (for which no preimage is known), it is computationally infeasible to find any input x s.t. h(x) = y

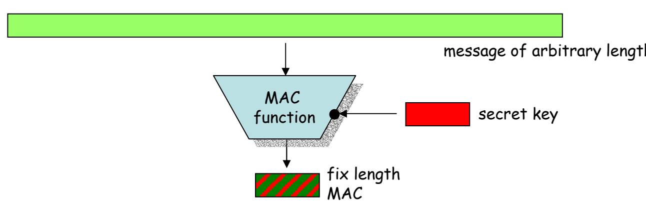
Iterated hash functions

- input is divided into fixed length blocks
- last block is padded if necessary
- each input block is processed according to the following scheme

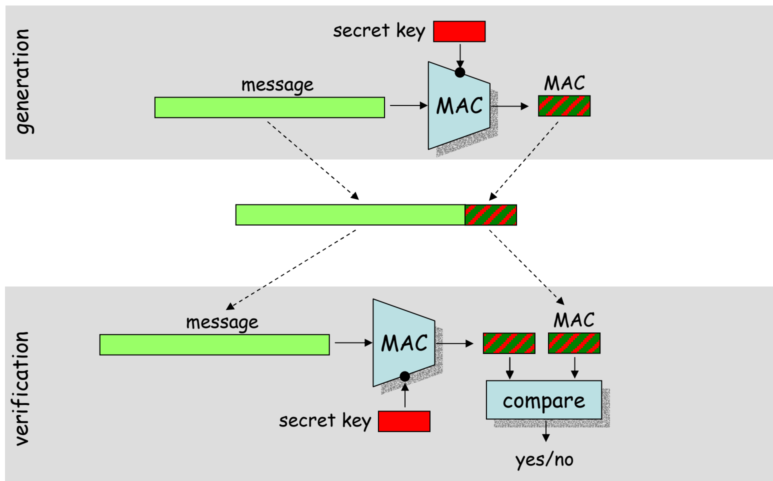


Message authentication codes (MACs)

- MAC functions can be viewed as hash functions with two functionally distinct inputs: a message and a secret key
- they produce a fixed size output (say n bits) called the MAC
- practically it should be infeasible to produce a correct MAC for a message without the knowledge of the secret key
- MAC functions can be used to implement data integrity and message origin authentication services



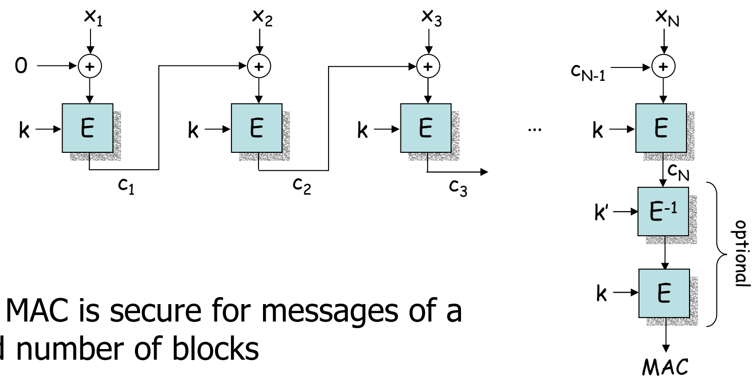
MAC generation and verification



Desirable properties of MAC functions

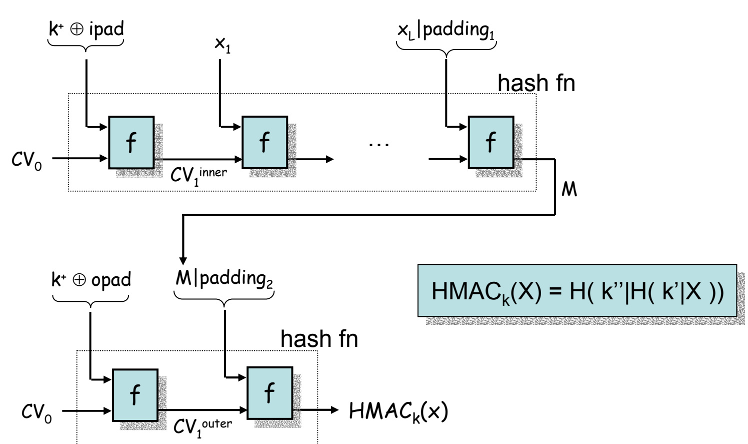
- ease of computation
  - given an input x and a secret key k, it is easy to compute $MAC_k(x)$
- key non-recovery
  - it is computationally infeasible to recover the secret key k, given one or more text-MAC pairs $(x_i, MAC_k(x_i))$ for that k
- computation resistance
  - given zero or more text-MAC pairs $(x_i, MAC_k(x_i))$, it is computationally infeasible to find a text-MAC pair $(x, MAC_k(x))$ for any new input $x \neq x_i$
  - computation resistance implies key non-recovery but the reverse is not true in general

CBC MAC



- CBC MAC is secure for messages of a fixed number of blocks
- (adaptive chosen-text existential) forgery is possible if variable length messages are allowed

HMAC

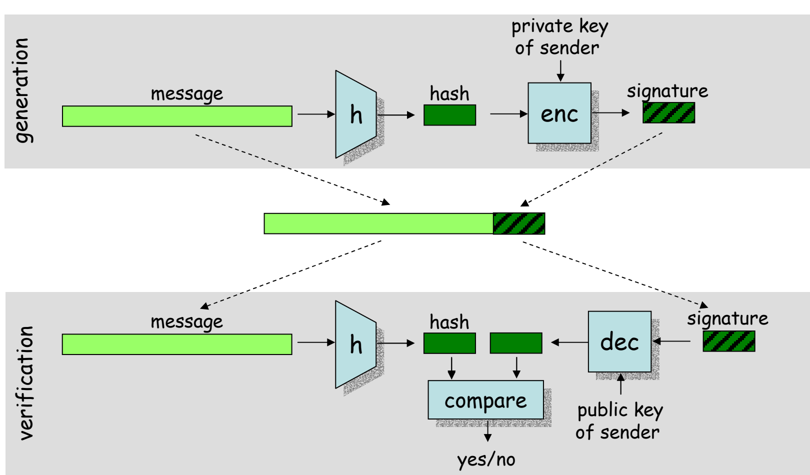


Digital signatures

- similar to MACs but
  - unforgeable by the receiver
  - verifiable by a third party
- used for message authentication and non-repudiation (of message origin)
- based on public-key cryptography
  - private key defines a signing transformation S_A
    - $S_A(m) = \sigma$
  - public key defines a verification transformation V_A
    - $V_A(m, \sigma)$ = true if $S_A(m) = \sigma$
    - $V_A(m, \sigma)$ = false otherwise

"Hash-and-sign" approach

- public/private key operations are slow
- hash the message first and apply public/private key operations to the hash value only



Key establishment protocols

- goal of key establishment protocols
  - to setup a shared secret between two (or more) parties
  - it is desired that the secret established by a fixed pair of parties varies on subsequent executions of the protocol (dynamicity)
  - established shared secret is used as a *session key* to protect communication between the parties

- motivation for use of session keys
  - to limit available ciphertext for cryptanalysis
  - to limit exposure caused by the compromise of a session key
  - to avoid long-term storage of a large number of secret keys (keys are created on-demand when actually required)
  - to create independence across communication sessions or applications

Basic classification

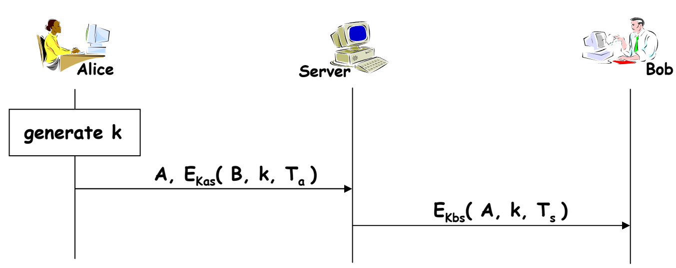
- key transport protocols
  - one party creates or otherwise obtains a secret value, and securely transfers it to the other party

- key agreement protocols
  - a shared secret is derived by the parties as a function of information contributed by each, such that no party can predetermine the resulting value

Further services

- entity authentication
- implicit key authentication
  - one party is assured that no other party aside from a specifically identified second party (and possibly some trusted third parties) may gain access to the established session key
- key confirmation
  - one party is assured that a second (possibly unidentified) party actually possesses the session key
  - possession of a key can be demonstrated by
    - producing a one-way hash value of the key or
    - encryption of known data with the key
- key freshness
  - one party is assured that the key is new (never used before)

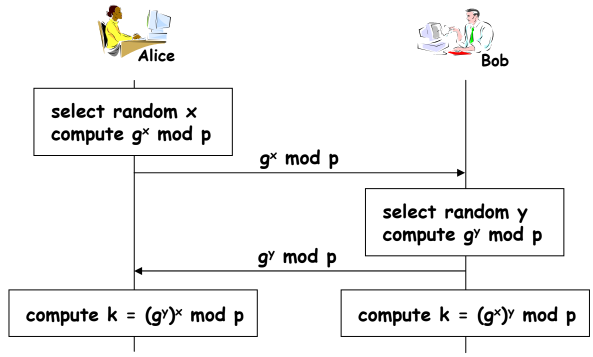
The Wide-Mouth-Frog protocol



protocol characteristics:

key transport protocol
implicit key authentication for Alice
explicit key authentication for Bob
key freshness for Bob (based on timestamps) **FLAWED !!!**
unilateral entity authentication of Alice
on-line third party (Server) trusted for secure relaying of keys and verification of freshness,
in addition A is trusted for generating good keys
initial long-term keys between the parties and the server are required

The Diffie-Hellman protocol



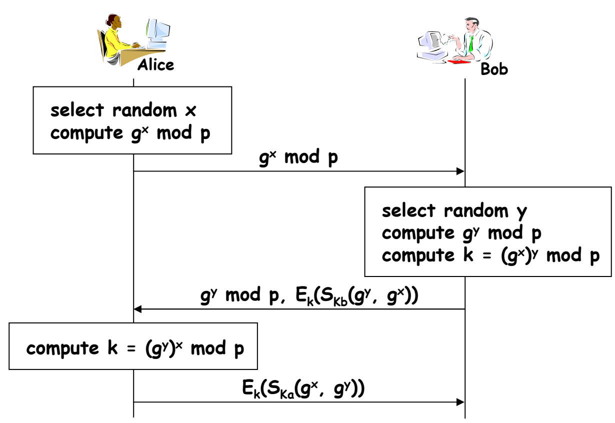
assumptions:

p is a large prime, g is a generator of Z_p^*,
both are publicly known system parameters

protocol characteristics:

key-agreement protocol
NO AUTHENTICATION
key freshness (randomly selected exponents)
no need for an (online) trusted third party

The Station-to-Station protocol



protocol characteristics:

mutual explicit key authentication (digital signatures,
usage of the session key)
key freshness (random exponents)
off-line third party for issuing public key certificates is required
initial exchange of public keys between the parties may be required

Summary

- security is about how to prevent attacks, or – if prevention is not possible – how to detect attacks and recover from them
- an attack is a a *deliberate attempt* to compromise a system
- security is provided in form of security services that are implemented by using security mechanisms
- many security mechanisms are based on cryptography (e.g., encryption, digital signature, some data integrity mechanisms, some authentication schemes, etc.)

Security and Privacy in Upcoming Wireless Networks

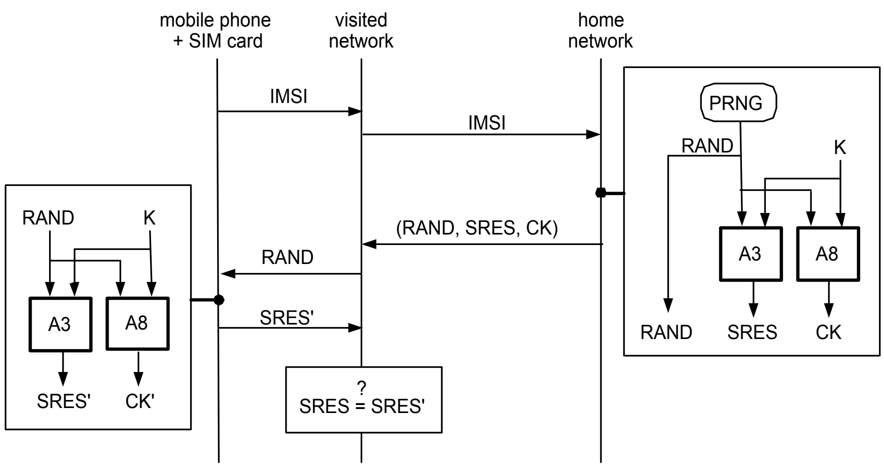
Security in existing wireless networks

GSM security;
WiFi security;

GSM security

- main security requirement
  - subscriber authentication (for the sake of billing)
    - cryptographic challenge-response protocol
    - long-term secret key shared between the subscriber and the home network operator
    - supports roaming without revealing long-term key to the visited networks
- other security services provided by GSM
  - confidentiality of communications and signaling over the wireless interface
    - encryption key shared between the subscriber and the visited network is established with the help of the home network as part of the subscriber authentication protocol
  - protection of the subscriber's identity from eavesdroppers on the wireless interface
    - usage of short-term temporary identifiers

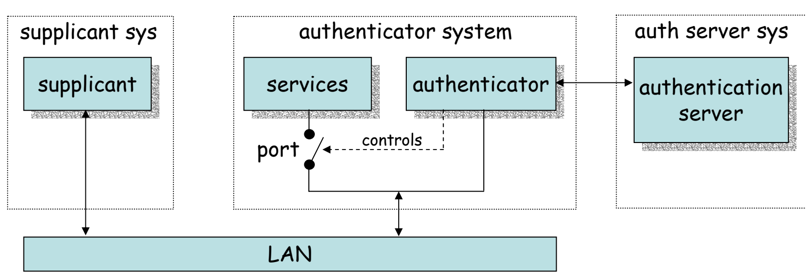
GSM authentication protocol



WiFi security

- security services
  - access control to the network
  - message confidentiality and integrity between the mobile station and the access point
- early solution was based on WEP
  - seriously flawed, not recommended to use
- the new security standard for WiFi is 802.11i
  - access control model is based on 802.1X
  - flexible authentication based on EAP and upper layer authentication protocols (e.g., TLS, GSM authentication)
  - improved key management
  - message protection protocols: TKIP (WPA) and AES-CCMP (WPA2)
  - TKIP
    - uses RC4
    - runs on old WEP hardware, but corrects WEP's flaws
  - AES-CCMP
    - uses AES in CCMP mode (CTR mode and CBC-MAC)
    - needs new hardware that supports AES

802.1X authentication model



- the supplicant requests access to the services (wants to connect to the network)
- the authenticator controls access to the services (controls the state of a port)
- the authentication server authorizes access to the services
  - the supplicant authenticates itself to the authentication server
  - if the authentication is successful, the authentication server instructs the authenticator to switch the port on
  - the authentication server informs the supplicant that access is allowed

Mapping the 802.1X model to WiFi

- supplicant → mobile device (STA)
- authenticator → access point (AP)
- authentication server → server application running on the AP or on a dedicated machine
- port → logical state implemented in software in the AP

- one more thing is added to the basic 802.1X model in 802.11i:
  - successful authentication results not only in switching the port on, but also in a session key between the mobile device and the authentication server
  - the session key is sent to the AP in a secure way
    - this assumes a shared key between the AP and the auth server
    - this key is usually set up manually

Protocols – EAP, EAPOL, and RADIUS

- EAP (Extensible Authentication Protocol) [RFC 3748]
  - carrier protocol designed to transport the messages of "real" authentication protocols (e.g., TLS)
  - very simple, four types of messages:
    - EAP request – carries messages from the supplicant to the authentication server
    - EAP response – carries messages from the authentication server to the supplicant
    - EAP success – signals successful authentication
    - EAP failure – signals authentication failure
  - authenticator doesn't understand what is inside the EAP messages, it recognizes only EAP success and failure

- EAPOL (EAP over LAN) [802.1X]
  - used to encapsulate EAP messages into LAN protocols (e.g., Ethernet)
  - EAPOL is used to carry EAP messages between the STA and the AP

- RADIUS (Remote Access Dial-In User Service) [RFC 2865-2869, RFC 2548]
  - used to carry EAP messages between the AP and the auth server
  - MS-MPPE-Recv-Key attribute is used to transport the session key from the auth server to the AP
  - RADIUS is mandated by WPA and optional for RSN

Summary

- authentication and key establishment protocols use (online) trusted third parties
  - Home Network (GSM)
  - Authentication Server (WiFi)
- trust is based on long-term relationships (established by contracts) and represented by long-term keys
- communication security measures are restricted to a single wireless hop
  - mobile phone – base station (GSM)
  - mobile station – access point (WiFi)
- privacy is not seriously protected

Upcoming wireless networks and new challenges

upcoming wireless networks:
- mesh networks,
- ad hoc networks,
- sensor networks,
- vehicular networks,
- RFID/NFC systems;

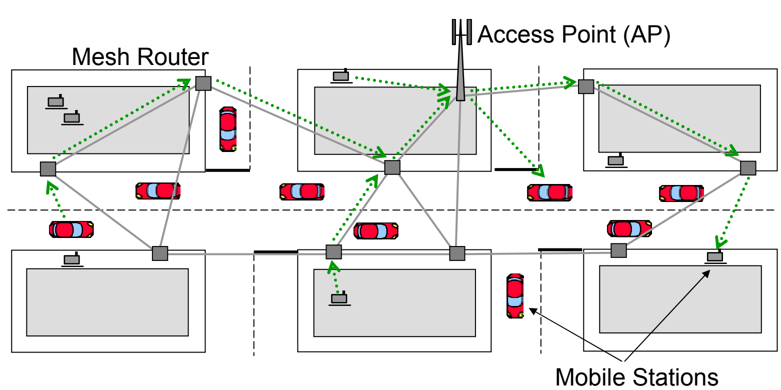
new challenges for security and privacy;

Upcoming wireless networks

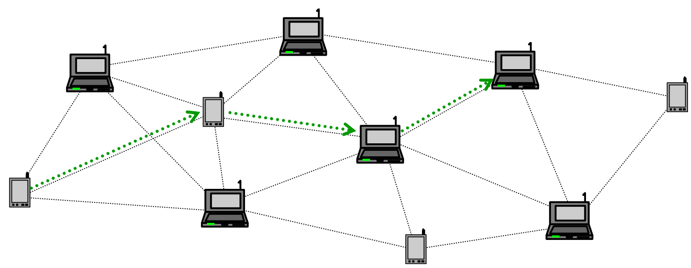
- everything beyond current wireless networks (3G and WiFi)
- examples:
  - wireless mesh networks (operator or community based)
  - infrastructureless ad hoc networks
  - vehicular communication systems
  - wireless sensor networks
  - RFID/NFC systems
  - personal area networks
  - body area networks
  - …

Wireless mesh networks

- mesh technology can be used to extend the coverage of wireless hot spots in a sizeable geographical area
  - Internet connectivity is provided to a larger population at a lower cost
- based on transit access points (mesh routers) and multi-hop wireless communications



Infrastructureless ad hoc networks



- infrastructureless operation = merging terminal and router functions
- nodes are potentially mobile
- application areas:
  - battlefield communications (and rescue operations)
  - free-of-charge personal communications
  - wireless embedded system (body area networks, networks of houshold appliances, vehicular ad hoc networks, ...)
- similar trend at the application layer is called peer-to-peer computing

Vehicular communications – motivation

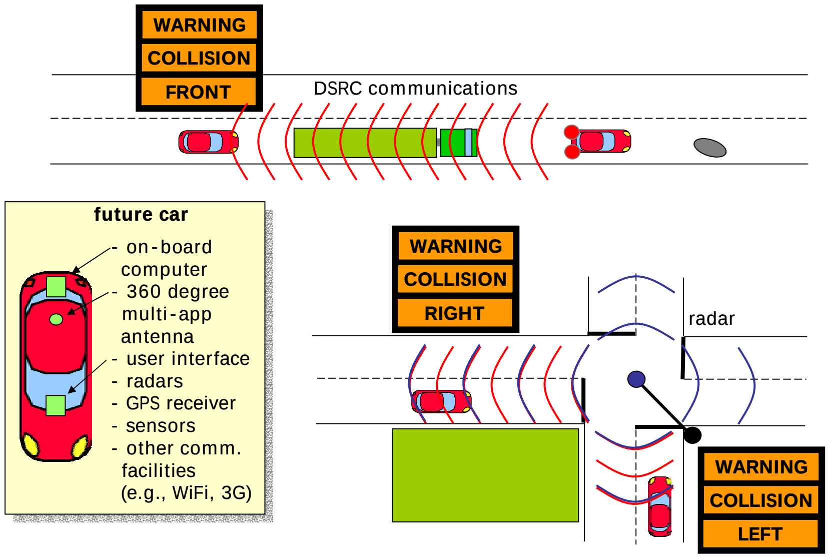
- side effects of road traffic

40000 people die and 1.5 million are injured every year in the EU

traffic jams generate a tremendous waste of time and fuel

- most of these problems could be solved by providing appropriate information to the driver or to the vehicle

Vehicular communications – examples (C2C and I2C)

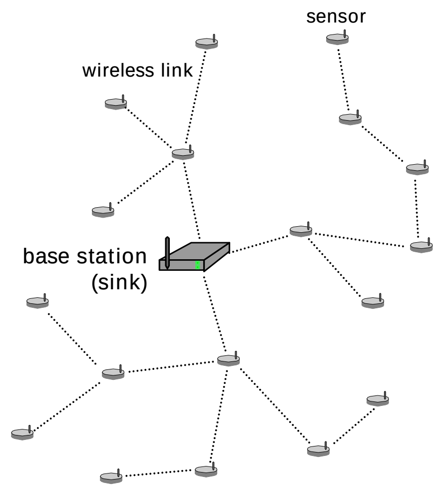


Envisioned VC applications for public safety

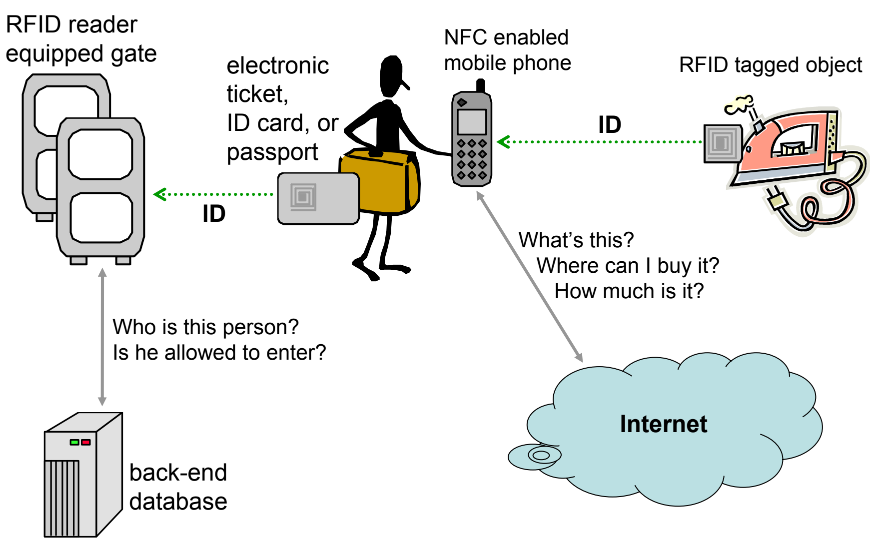
- APPROACHING EMERGENCY VEHICLE (WARNING) ASSISTANT (3)
- EMERGENCY VEHICLE SIGNAL PREEMPTION
- ROAD CONDITION WARNING
- LOW BRIDGE WARNING
- WORK ZONE WARNING
- IMMINENT COLLISION WARNING (D)
- CURVE SPEED ASSISTANCE [ROLLOVER WARNING] (1)
- INFRASTRUCTURE BASED – STOP LIGHT ASSISTANT (2)
- INTERSECTION COLLISION WARNING/AVOIDANCE (4)
- HIGHWAY/RAIL [RAILROAD] COLLISION AVOIDANCE (10)
- COOPERATIVE COLLISION WARNING [V-V] (5)
- GREEN LIGHT - OPTIMAL SPEED ADVISORY (8)
- COOPERATIVE VEHICLE SYSTEM – PLATOONING (9)
- COOPERATIVE ADAPTIVE CRUISE CONTROL [ACC] (11)
- VEHICLE BASED PROBE DATA COLLECTION (B)
- INFRASTRUCTURE BASED PROBE DATA COLLECTION
- INFRASTRUCTURE BASED TRAFFIC MANAGEMENT – [DATA COLLECTED from] PROBES (7)
- TOLL COLLECTION
- TRAFFIC INFORMATION (C)
- TRANSIT VEHICLE DATA TRANSFER (gate)
- TRANSIT VEHICLE SIGNAL PRIORITY
- EMERGENCY VEHICLE VIDEO RELAY
- MAINLINE SCREENING
- BORDER CLEARANCE
- ON-BOARD SAFETY DATA TRANSFER
- VEHICLE SAFETY INSPECTION
- DRIVER'S DAILY LOG

Wireless sensor networks

- environmental monitoring (for ecological and/or agricultural purposes)
- monitoring the state of structures (e.g., bridges, tunnels, …)
- remote patient monitoring (elderly and chronically ill people)
- industrial process automation
- building automation
- …
- military applications



RFID/NFC systems



Challenges for providing security

- multi-hop wireless communications
  - why?
    - reduce interference
    - reduce energy consumption
    - save on infrastructure deployment
  - consequences
    - terminals play the role of network nodes (routers)
    - where's the edge of the network?
- lack of physical protection
  - why?
    - unattended operation
    - no tamper resistance (it would cost a lot)
  - consequences
    - easy access to devices
    - nodes may be compromised

Hacking your Prius [CNET News.com]

More challenges (1/2)

- scale
  - thousands or millions of nodes (e.g., Smart Dust)
  - network is not necessarily hierarchically organized
  - or hierarchy is built on-the-fly
- mobility
  - dynamically changing topology
  - intermittent connectivity
  - transient relationships
- self-organization
  - infrastructureless operation
  - decentralization

More challenges (2/2)

- increased programmability of devices
  - easy to install new applications
  - basic operation of the device can be modified (e.g., software defined radio)
- resource constraints
  - tiny, embedded devices, running on batteries
  - no support for heavy cryptographic algorithms
  - energy consumption is an issue
- embedded systems
  - many nodes are not directly operated by humans
  - decisions must be made autonomously
- increased privacy risks
  - many wireless devices are carried by people or embedded in vehicles
  - easy tracking of whereabouts of individuals

Trust

- the trust model of current wireless networks is rather simple
  - subscriber – service provider model
  - subscribers trusts the service provider for providing the service, charging correctly, and not misusing transactional data
  - service providers usually do not trust subscribers, and use security measures to prevent or detect fraud
- in the upcoming wireless networks the trust model will be much more complex
  - entities play multiple roles (users can become service providers)
  - number of service providers will dramatically increase
  - user – service provider relationships will become transient
- how to build up trust in such a volatile and dynamic environment?
- yet, trust is absolutely fundamental for the future of wireless networks
  - pervasiveness of these technologies means that all of us must rely on them in our everyday life!

Reasons to trust

- moral values
  - it will be difficult to observe compliance with them
- experience about another party
  - relationships may not last long enough for this
- rule enforcement organizations
  - need to rely more on rule enforcement mechanisms
- **rule enforcement mechanisms**
  - prevent bad things from happening → security techniques
  - encourage desirable behavior → game theory and mechanism design

Summary

- upcoming wireless networks are very different from existing wireless networks
- traditional approaches to security are not applicable in many cases
- risk of privacy violation is increased
- the field of security and privacy in upcoming wireless networks is full of challenging research topics