WiFi
Basics & Security

original slides by
Matthias Vallentin
vallentin@net.in.tum.de

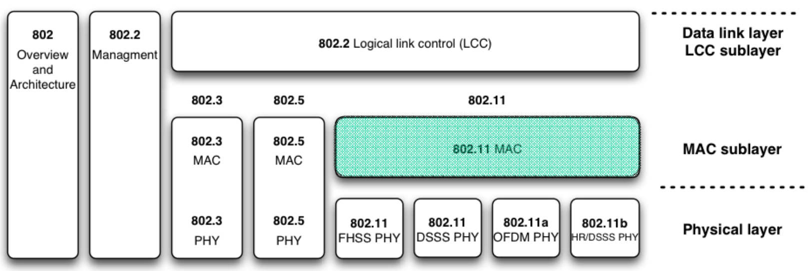
1

Outline

- 802.11 ("WiFi") Basics
  - Standards: 802.11{a,b,g,h,i}
  - CSMA/CA
- WiFi Security
  - WEP
  - 802.11i
  - DoS

2

IEEE 802 family



3

802.11 standards

1. 802.11 Basics
2. Standards
3. CSMA/CA

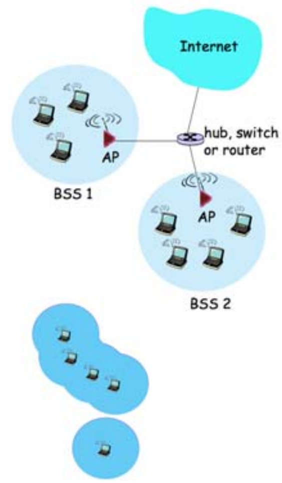
	802.11	802.11b	802.11a /h	802.11g	802.11n
Year	1997	1999	1999/2002	2003	vorauss. Ende 2006
Frequency	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz	5 GHz
Transfer rate	2 MBit/s	11 MBit/s	54 MBit/s	54 MBit/s	~600 MBit/s
Acceptance	veraltet	stark verbreitet	gering	verbreitet	-
Security	-	WEP	WEP	WEP, WPA	

802.11i is an **Amendment**

4

802.11 operational modes

- Infrastructure mode
  - Access Point (AP) interface to wired network
  - Basic Service Set (BSS) contains
    - Wireless hosts
    - Access Point (ad hoc mode: only hosts)
- Ad hoc mode
  - no access points
  - nodes can only transmit to other nodes within link coverage
  - nodes organize themselves



5

Wireless link characteristics

Differences to wired link ….

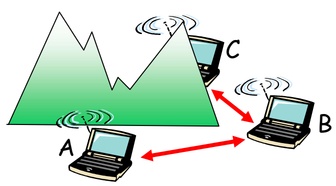
- Decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- Interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- Multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more "difficult"

6

Wireless network characteristics

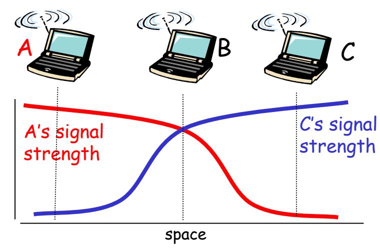
Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other

means A, C unaware of their interference at B



Signal fading:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interferring at B

7

IEEE 802.11 multiple access

- 802.11 Carrier Sense Mulitple Access – "listen" before sending
  - to avoid collisions with ongoing transmissions
- 802.11: no Collision Detection (CD)!
  - would require parallel sending (own data) und receiving (sensing collisions) → expensive!
  - Not all collisions can be detected anyhow → hidden node, signal fading
- Goal: avoid collisions:
  - CSMA/C(ollision)A(voidance)

8

802.11 MAC Protocol: CSMA/CA

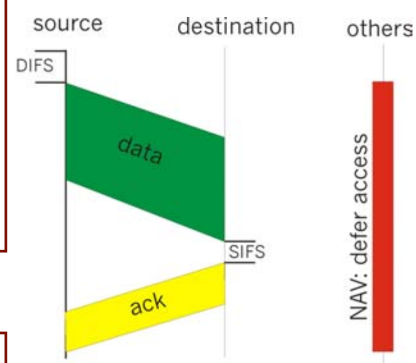
- 802.11 Sender

```
1 if (sense channel idle for DIFS)
        transmit entire frame (no CD)
2 if (sense channel busy) {
        start random backoff timer
        timer counts down while channel idle
        transmit when timer expires
        if (no ACK) {
            increase random backoff interval
            repeat 2
        }
}
```

- 802.11 Empfänger

```
if (frame received OK)
        return ACK after SIFS

ACK necessary due to hidden terminal problem
```



9

Avoiding collisions (more)

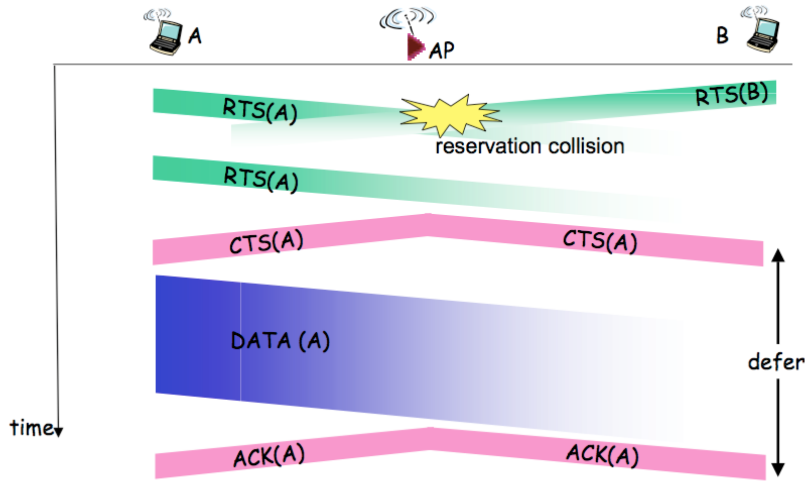
idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- RTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

Avoid data frame collisions completely using small reservation packets!

10

CSMA/CA: RTS-CTS exchange



11

Outline

- 802.11 ("WiFi") Basics
  - Standards: 802.11{a,b,g,h,i}
  - CSMA/CA
- WiFi Security
  - WEP
  - 802.11i
  - DoS

12

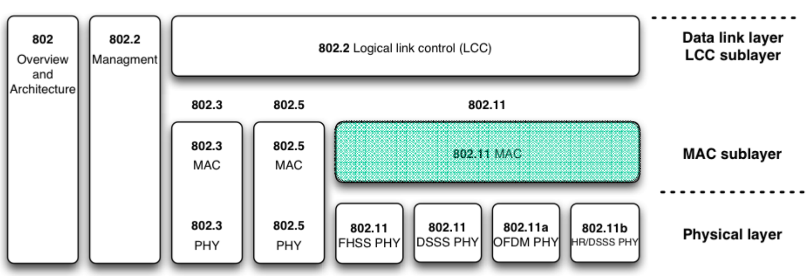
WiFi security

- Wireless security
  - Confidentiality
  - Authenticity
  - Integrity
  - Availability

- Do the existing security protocols (WEP, WPA, WPA2) address these aspects?

13

IEEE 802 Familie



14

Wired Equivalent Privacy (WEP)

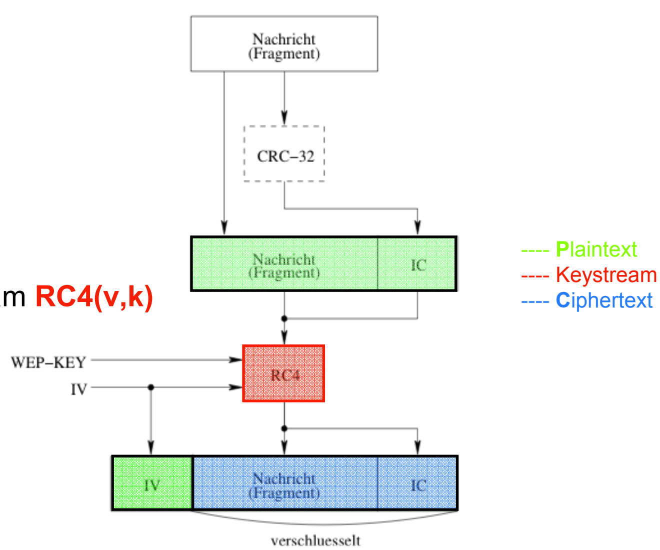
- Part of the 802.11 standard
  - Goal: secure the MAC layer
- Design goals:
  - **Confidentiality**
  - **Access Control**
  - **Data Integrity**: via checksum (CRC32)
- *Stream Cipher*
  - **RC4** ("*arcfour*")
  - Input-Parameters:
    - initialization vector **v** and secure key **k**
    - Key stream: **RC4(v,k)** (**v** is also known as *seed*)

100
□
010
=
110

15

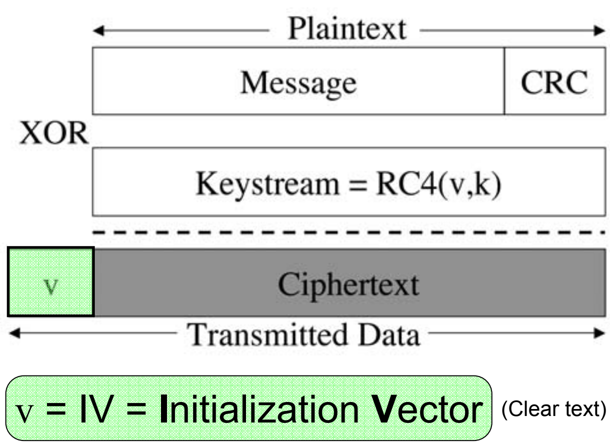
WEP

Keystream **RC4(v,k)**



16

WEP (2)



17

Attacks on WEP

- Bruteforce
- Key stream reuse
  - IV dictionary
- Weak IVs
- Frame injection
- Fragmentation attack

18

Key stream reuse

- Reuse of an already used key stream RC4(v,k)
- Key stream space: **24 bit = 2^{24} IVs**
- Attacker can decode packets encrypted with the same key stream
- With even just one valid key stream an attacker can send arbitrary frames into the network
  - 802.11b has no protection against *replay attacks*

RC4(v,k) □ **P**laintext = **C**iphertext

19

Key stream reuse (2)

- **IV dictionary:** stores all IVs together with their corresponding key stream
- With a full dictionary an attacker can decode all traffic
- How to get valid key streams?
  - *Shared Key Authentication* (deprecated)
  - *Known plaintext*
  - *Fragementation attack*
    - Relaying broadcast frames
    - *Chop-Chop* (key stream "guessing")

RC4(v,k) = **P** □ C

20

Weak IVs

- Private key ***k*** computable
  - **"weak" IVs**: reveal a byte of the private key ***k***
  - Known RC4 weakness
  - 4 years (!) prior to the publication of WEP
- Vendors offered hardware patches: filter weak IVs
  - Aggravates problem: reduces key stream space: $< 2^{24}$
  - Legacy host can compromise whole network

21

Frame injection

- Additional classes of weak IVs are known
  - Up to 13% reveal a key byte
- Vendor decided to ignore it (no further IV-filters)
  - Still needs ≈ 500.000 - 1.000.000 packets for successful attack => "long" waiting times
- Speedup of attack possible via WEP frames replay
  - Only frames that imply an answer e.g.: ARP request (recognizable via fixed size)
- Vendor solution: EAP with fast re-keying
  - EAP = Extensible Authentication Protocol
    - Authentication Framework, no special authentication mechanism
    - ca. 40 methods: EAP-MD5, EAP-OTP, EAP-GTP, ... , EAP-TLS, ...

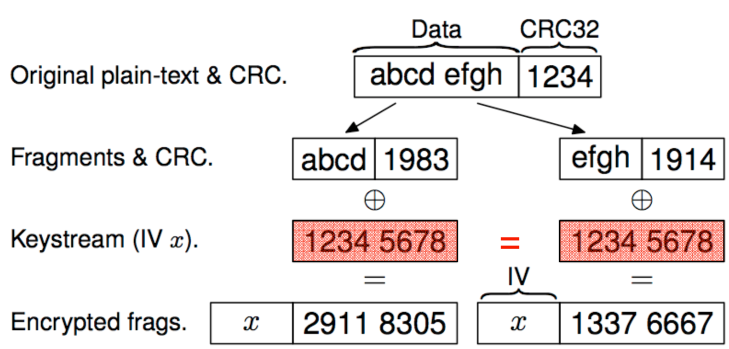
22

Fragmentation attack

- New real-time attack, robust against frequent re-keying enables
  - Sending of data into WEP network
  - Decryption of WEP data
- Approach: 802.11 can be used against WEP ☠
  - 802.11 specifies fragmentation on MAC layer
    - Each fragment is individually encrypted
    - Multiple fragments can be send with the same key stream
    - Max. 16 fragments, due to 4 bit field for FragNo

23

802.11 Fragmentation



24

Fragmentation attack (2)

- **8** bytes of known plaintext in each frame*
  - 802.11 Frames use **LLC/SNAP** encapsulation (constant/known header)

0xAA	0xAA	0x03	0x00	0x00	0x00	0x08	??
DSAP	SSAP	CTRL	ORG code			Ether type	

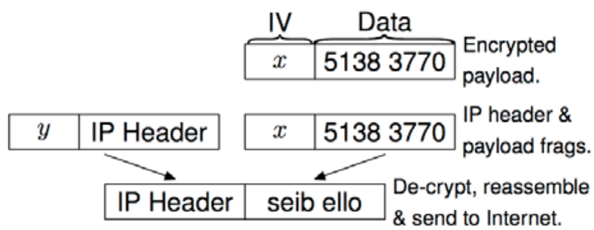
  - Ether type = IP or ARP
  - => 8 bytes of key stream are known
    - **P** □ **C** = RC4(v,k)
- (8 - 4) x 16 = 64 bytes data can be injected immediately via fragmentation
  - 4 bytes for CRC (therefore 8 - 4)

Fragmentation attack (3)

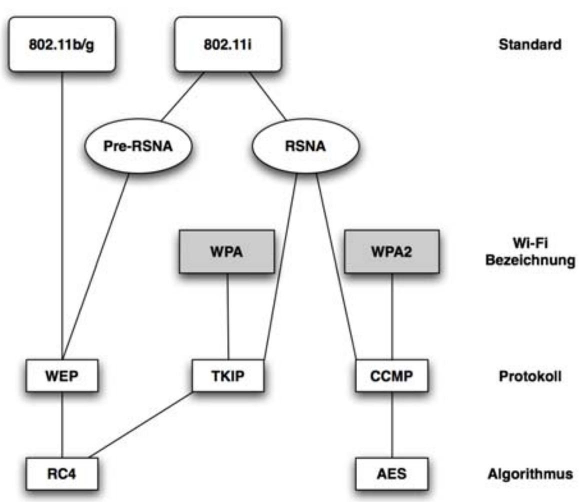
- Why does it help?
  - Can speedup other attacks (e.g.: weak IV)
  - Key stream attacks
    - determine 8 bytes of key stream
    - extend key stream: send long broadcast frames in several fragments and decode answers from AP (C □ P = RC4(v,k)). Repeat until 1500 bytes (MTU) of the key stream are known
    - IV Dictionary:
      - Send 1500 byte broadcasts
      - AP is likely to rely packet
      - Determine key stream for this packet and via this all further key streams
    - Decode packets with known key streams
  - Decode packets in real-time...

Fragmentation attack (4)

- Decoding of packets in *real-time*
  - Requirement: Internet connectivity
  - Attacker can use AP for decoding ☠
  - With 802.11 fragmentation one can add an additional IP-header in front of the original packet
  - Original packet is contained in last fragment
    - AP reassembles, decodes the packet and sends it to the spoofed IP address



802.11 termini



802.11 security

	WEP	WPA	WPA2
Algorithm	RC4	RC4	AES-CTR
Key length	64/128 bit	128 bit	128 bit
IV-length	24 bit	48 bit	48 bit
Data integrity	CRC-32	Michael	CBC-MAC
Header integrity	-	Michael	CBC-MAC
Authentication	Shared Key	802.1X	802.1X
Key-management	-	802.1X	802.1X
Replay-attack protection	-	IV-Sequenz	IV-Sequenz

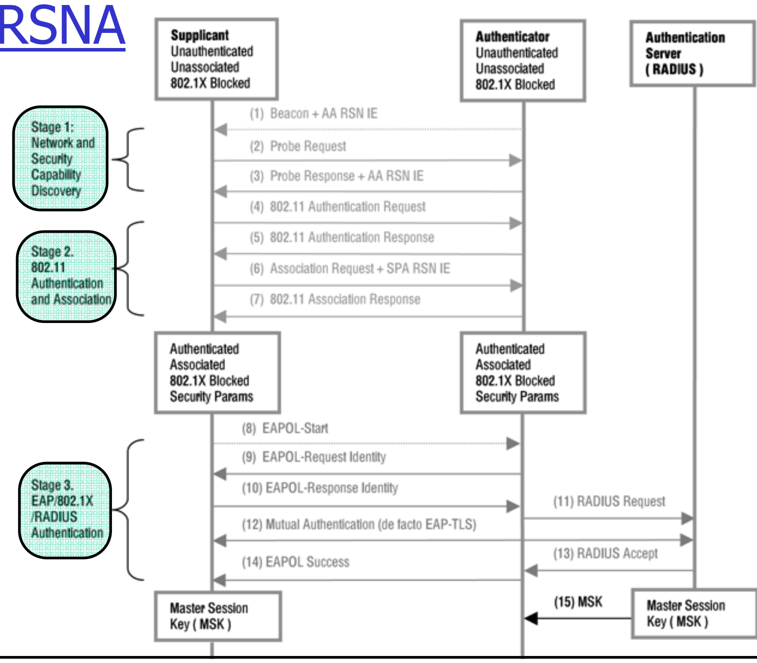
29

802.11i - RSNA overview

- 3 entities for Robust Security Network Association (RSNA)
  - Supplicant (WLAN client)
  - Authenticator (access point)
  - Authentication server (almost always a RADIUS server)
- 6 connection phases until data exchange
  - Phase 1: Network and Security Capability Discovery
  - Phase 2: 802.11 Authentication and Association
  - Phase 3: EAP/802.1X/RADIUS Authentication
  - Phase 4: 4-Way Handshake
  - Phase 5: Group Key Handshake
  - Phase 6: Secure Data Communication
- More complex than WEP (luckily its also saver :)

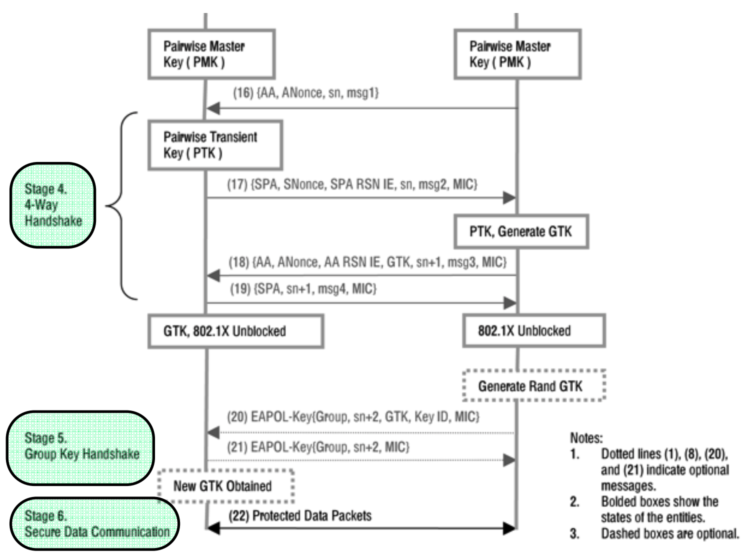
30

RSNA



31

RSNA (2.)



32

802.11i weaknesses

- PSK dictionary brute force attack
- Security level rollback attack
- Reflection attack

33

802.11i PSK brute force

- PSK = PMK = PBKDF2 (passphrase, SSID, SSIDlength, 4096, 256)

- PSK = Pre-Shared Key
- PMK = Pairwise Master Key
- PBKDF2 = methods from PKCS#5 v2.0
- SSID = Service Set Identity
- SSIDlength = length of the SSID
- 4096 = number of hashes
- 256 = output length

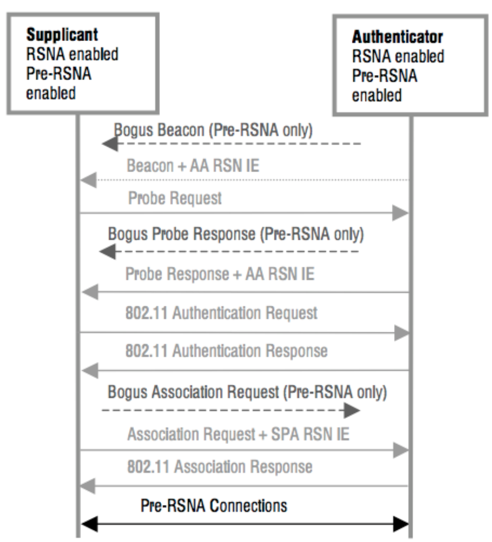
34

Security level rollback attack

- Transient Security Network (TSN): Compatibility modus for heterogeneous environments
  - Idea: use for soft migration to WPA2
  - Enables Pre-RSNA and RSNA connections
- Attacker simulates a Pre-RSNA authenticator
  - Send spoofed Probe-Requests / Beacons
  - Security reduces to the weakest component
  - Fallback to WEP :(

35

Security level rollback attack



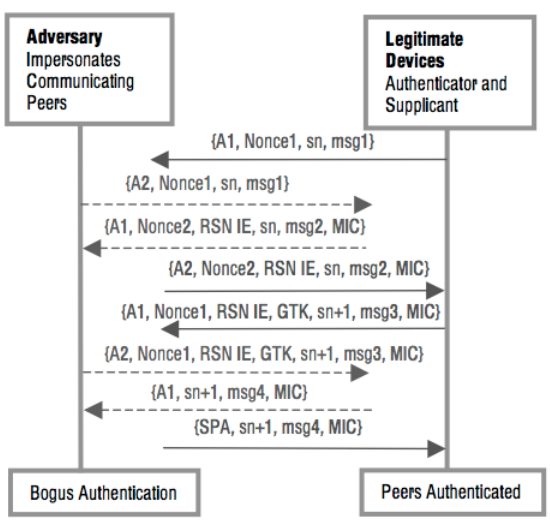
36

Reflection attack

- Attacker is Supplicant and Authenticator in one node
  - 4-Way-Handshake (4WH) as authenticator
  - 4WH as Supplicant with same parameters
- Responses from second 4WH can be used as valid data for the first 4WH
  - No mutual authentication
  - Encrypted data can be saved (e.g.: for offline analysis)
- Attack only works in ad hoc mode
  - With infrastructure mode Supplicant and Authenticator are always different nodes

37

Reflection attack



38

Denial-of-Service (DoS)

- Frequency Jamming (PHY)
- Deauthentication/disassociation frame spoofing
- CMCA/CA – no protection for management frames
  - Ignore standard: e.g.: no "backoff"
  - Virtual carrier-sensing (RTS with large NAV)
- ARP-Cache poisoning
- 802.1X
  - EAP-{Start, Logoff, Failure} Spoofing
  - EAP identifier only 8 bit: send more than 255 Authentication Request at the same time
- ➡ DoS too easy (not addressed by 802.11i!)
- ➡ DoS attack can easy further attack (*Session-Hijacking*, *MitM*)

Conclusion

- WiFi is ubiquitär / *pervasive*
- Continuous improvements of the standards
- Security aspects
  - Shared medium (!)
  - Forget about WEP
  - Use secure protocols (SSH, IMAPS, HTTPS) over WLAN
  - Use good WPA/WPA2 pass phrases p ($p \notin$ dictionary)
  - DoS (still) too easy
  - If important use cable :)

Course overview

- Introduction
  - Attacks and threats, cryptography overview
  - Authentication (Kerberos, SSL)
- Applications
  - Web, email, ssh
- Lower layer network security
  - IPsec, firewalls, wireless
- Monitoring / information gathering
  - Intrusion detection, network scans
- Availability
  - Worms, denial of service, network infrastructure

41