

1. Soft Switch e.g. bkw

Smart Meter
Regulations

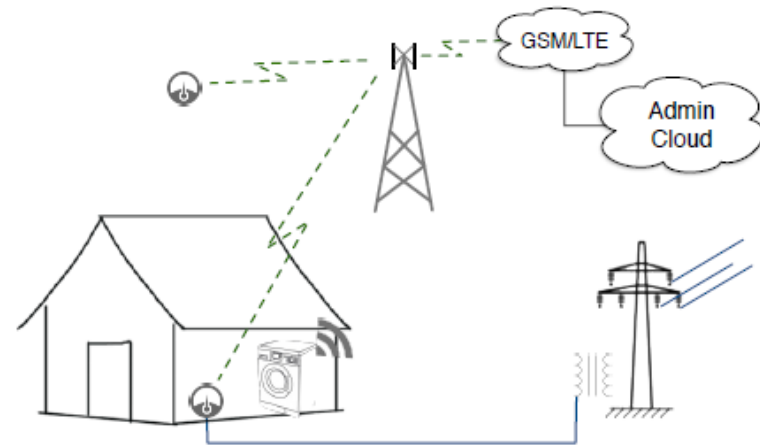
2. Remote Switch-off

On-place switch-on

3. Communicating

Application Scenarios for Smart Meters

- Monitoring the grid to achieve a grid stability of at least 99,96%,
- Alarm functionality, addressing
 - failure of components in the grid,
 - alarms related to the Smart Home, e.g. burglary, fire, or water leakage,
- Intrusion detection, monitoring both hacking attempts to the home as well as the control center and any entity in between,
- Billing functionality, providing at least the total consumption every hour, or even providing information such as max usage,
- Remote home control, interacting with e.g. the heating system
- Fault tolerance and failure recovery, providing a quick recovery from a failure.
- Future services
 - Monitoring of activity at home, e.g. “virtual fall sensor”



- Discuss with your neighbours

- Billing (1/hour) 1/min

→ Security, Privacy Goal: (s,p) -

Me Security DSO
70, 40, 80, 70
60 ↓

Privacy 90
65, 70, 60, 80

- Fire alarm ^{raise an alarm} _{not hampered by security}
→ Security, Privacy Goal: (s,p) -

availability broadcast "limit"
(20, 80, 95, 40) 10, 10, 0, 30
60

- Home Control (1/hour)

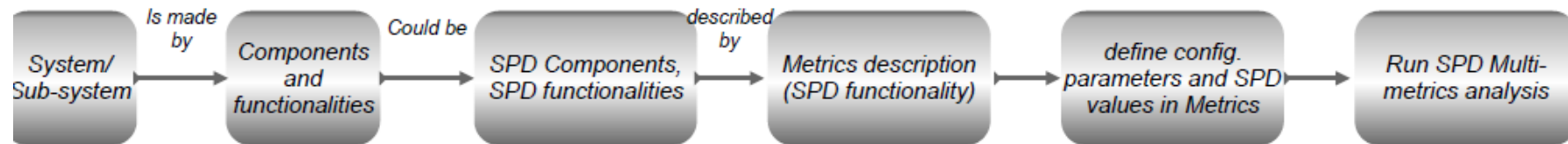
→ Security, Privacy Goal: (s,p) -

80, 80, 80, 80 70, 60, 80, 80

Privacy: 6y. 100
Prefers

Today
X YouTube 20
configurability

Methodology and AMR system: From System description to SPD level



- System: Automatic Meter System (AMS) consists of reader (AMR), aggregator, communications, storage, user access
- Sub-systems: AMR consists of power monitor, processing unit, communication unit
- Component: AMR communication contains of a baseband processing, antenna, wireless link
- Configuration Parameter: Wireless link: $f=868$ MHz, output power=?, Encryption=?



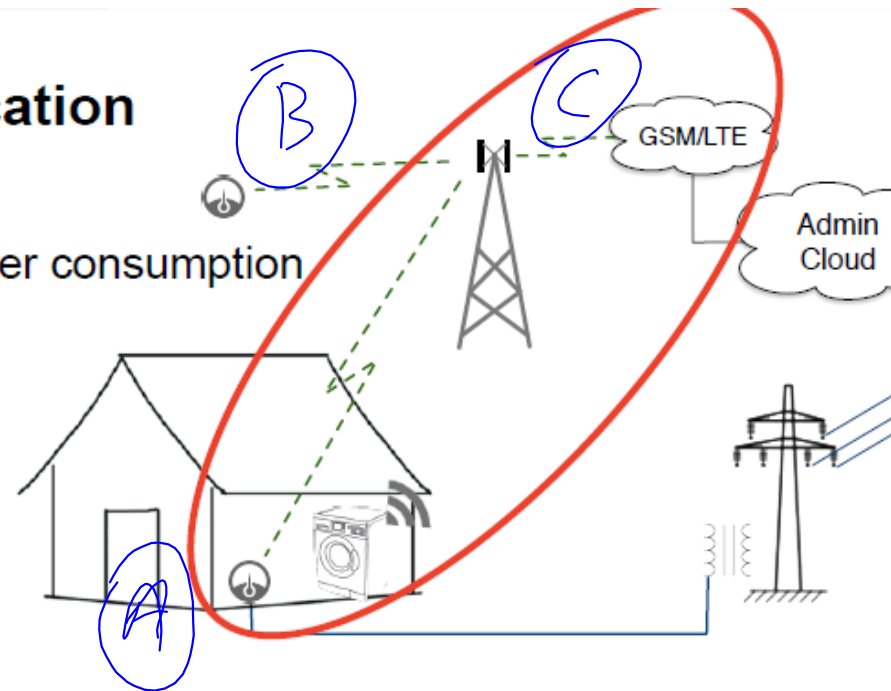
- Provide a list of Security/Privacy/Dependability Functionalities (e.g. encryption)

- Security management
Cryptography
trusted path
(tunnel) VPN
privacy
identification
authentication
upgradability
secure communication
accountability
authorization
integrity
Intr. detection system
user data protection
remote access
access control
transparency
certificates handling
secur
configurability
redundancy
resource utilization
Security updates
non-repudiation
resource management
phys. security

Sub-system analysis

here: Smart Meter with Communication

- the Automatic Meter Reader (AMR)
 - AMR to measure, sense and control power consumption
- the Mesh radio link
 - direct communication to concentrator
 - or multi-hop through other AMR
- the Mobile link sub-systems
 - from collector to mobile operator
 - typical 2G/3G/4G data, or SMS



Sub-system analysis Metrics for AMR

- the Automatic Meter Reader (AMR)
 - (1) remote access metric - (yes/no)
 - reading, or just controlling
 - (2) authentication metric
 - everyone, or authenticated user
 - (3) encryption metric (on, off)



(1) remote access

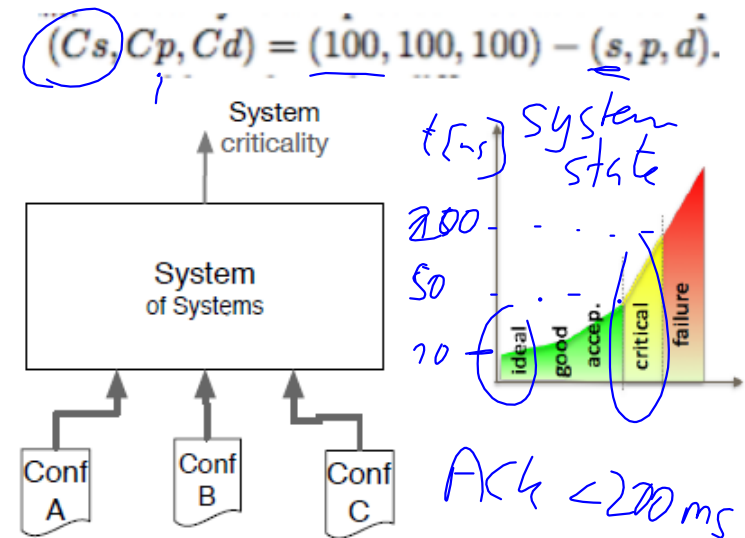
Configuration	Cs	Cp
Remote Access ON	60	60
Remote Access OFF	10	20

(2) authentication

Configuration	Cs	Cp
Authentication ON	10	30
Authentication OFF	80	70

(3) encryption

Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80



Metrics for Mesh Radio

- the Mesh radio link
 - (4) mesh
 - (5) message rate
 - (3) encryption

(3) encryption

Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80



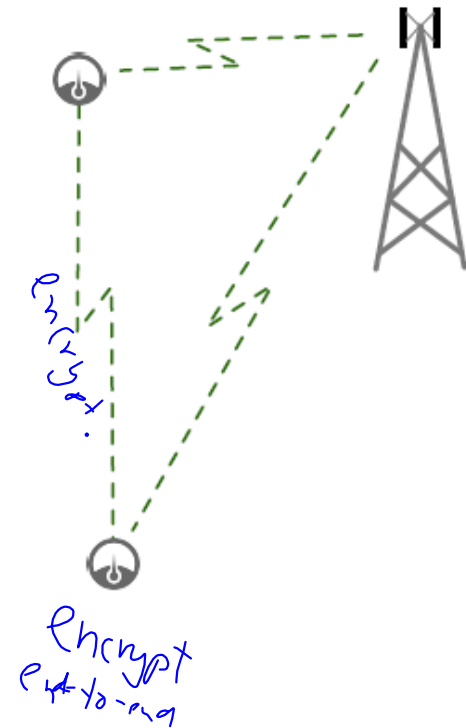
(4) mesh

Configuration	Cs	Cp
Multi-path routing	60	60
Single-path routing	30	30

(5) message rate

Configuration	Cs	Cp
1 hour	20	20
20 min	25	30
1 min	40	50
5 sec	50	70

UT

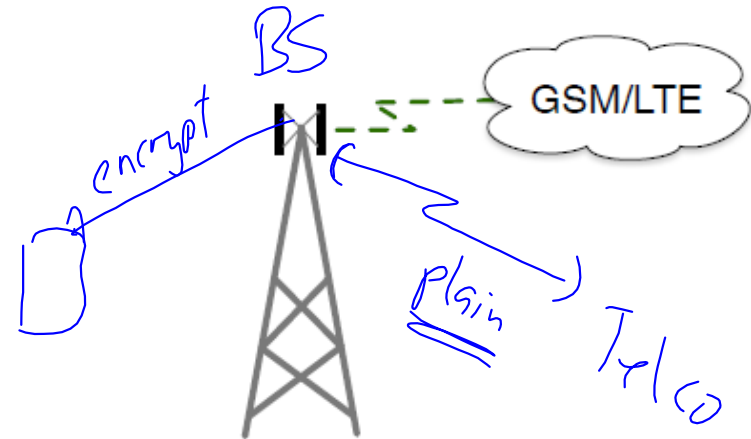


Mar2017, J. Noll, Gy. Kálmán

tricks for mobile link sub-system

the Mobile link sub-systems

- (6) mobile channel (2G or SMS)
- (6+) 3G/4G, IP, powerline
- (3) encryption



(3) encryption

Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80



(6) mobile channel

Configuration	Cs	Cp
GPRS	60	70
SMS	40	50

UMTS
4G

Multi-Metrics_{v2} - system composition

- System consists of sub-systems consists of components

→ security

→ privacy

→ dependability

W_S
 W_P
 W_D

Collector

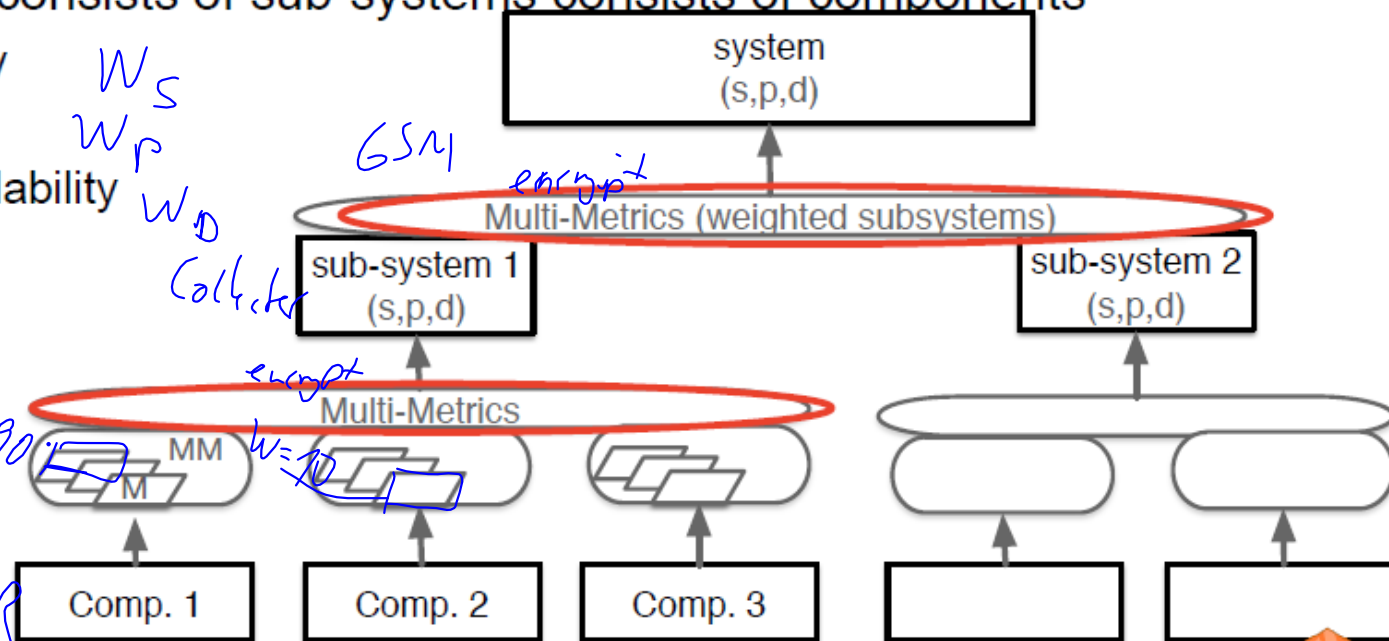
$w = 90$

except

$w = 10$



7/4/17



INIK4750 - Measurable Security

Mar2017 | Noll Gy. Kálmán



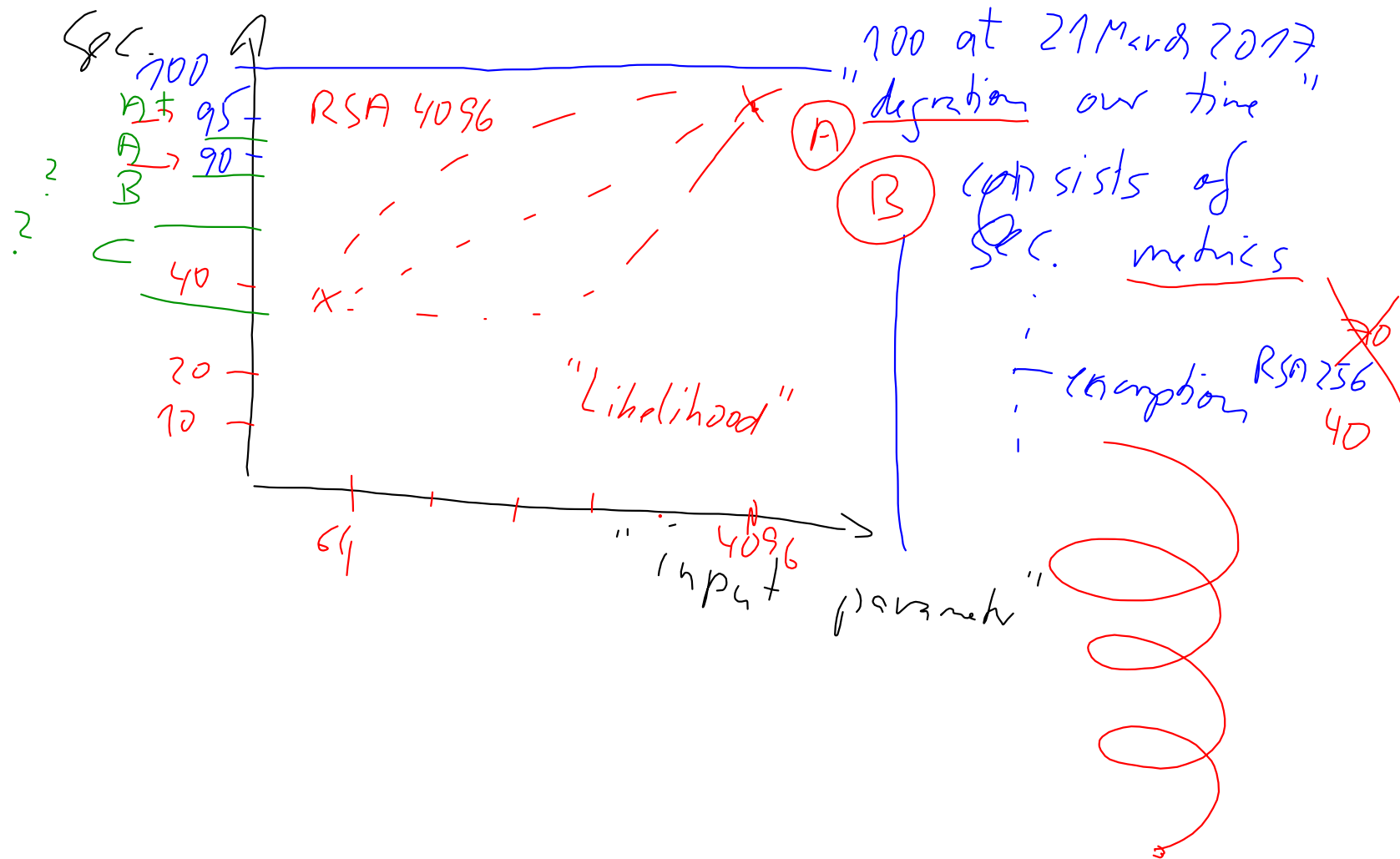
Weakness of the Multi-Metrics

a) S, P are subjective

90
80
⋮
20

b) weighting of metrics is subjective

c) "you never reach 100 in security"



s,p-goal versus system-s,p

- 11 possible configurations
 - selected as combinations of "states"
- highest SPD element dominates the outcome of the metrics
 - Billing & Home Control: security
 - Alarm: dependability

Sensitivity Analysis:

- max security: $s=84$
- same config: $p=77$

satisfies billing

(●, ●, ●)

satisfies home control

(●, ●, ●)



Goal

Table 1 SPD_{Goal} of es

Use Case	Security	Privacy
Billing	90	80
Home Control	90	80
Alarm	60	40

Table 9 Selected configuration SPD level for each use case

Use case	SPD _{Goal}	Configuration	SPD level	SPD vs SPD _{Goal}
Billing	(90,80,40)	10	(67,61,47)	(●, ●, ●)
Home Control	(90,80,60)	10	(67,61,47)	(●, ●, ●)
Alarm	(60,40,80)	6	(31,33,63)	(●, ●, ●)

11 23 11

urd

< 70

- Challenges

→ Logic: Centralised $\longleftrightarrow$ Fog, *Edge computing*

Smart Meter: Information $\longleftrightarrow$ Control

Smart Grid Information $\longleftrightarrow$ Internet Info



UNIK4750 - Measurable Security

Sub-system weighting

- Component criticality from metrics
- sub-system criticality from evaluation of components
- system criticality from evaluation of sub-systems
- Criticality C through root mean square weight
- Actual criticality x_i for component or (sub-)system
- Weight w_i for each metric,



Result will maximise the impact of high criticalities

$$C = \sqrt{\sum_i \left(\frac{x_i^2 W_i}{\sum_i W_i} \right)} \quad W_i = \left(\frac{w_i}{100} \right)^2$$

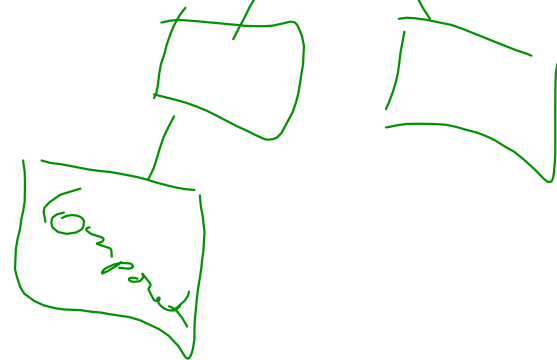
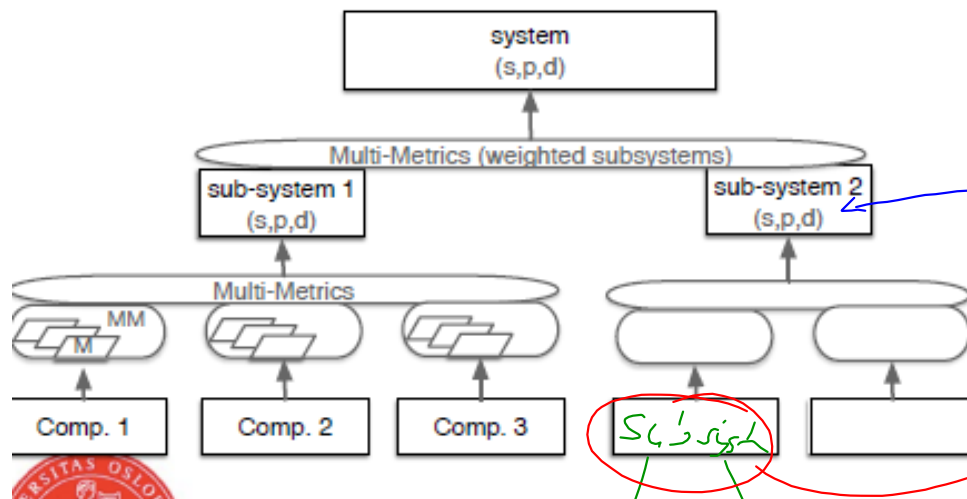
Table 8 Sub-systems and components weights

Sub-system	Sub-sys. Weight	Component	Comp. Weight
AMS	80	Remote Access	70
		Authentication	80
		Encryption	80
Radio link	50	Mesh	60
		Message Rate	80
		Encryption	40
Mobile link	20	Mobile link	70
		Encryption	40

Security

Sec. functions
Metrics 60
70

Sub system → AMR
Conf. A B C



max security
 given an application
 goal $S \Rightarrow 0$
 which configuration?
 bad apples?

n of

$$C = \sqrt{\sum_i \left(\frac{x_i^2 W_i}{\sum_i^n W_i} \right)} \quad W_i = \left(\frac{w_i}{100} \right)^2$$

Table 8 Sub-systems and components weights

1) $\sum$ weights = normalized

$\cdot w_1 = 70, 90, 85, 60$

2) why $()^2$ - Psychology

$\cdot w_2 = 30, 40, 35, 30$

Example: $w (0.2)^2 \cdot 40$

$0.04 \cdot 40 = 1.6$

Weight * Criticality = $(0.8)^2 \cdot 60$

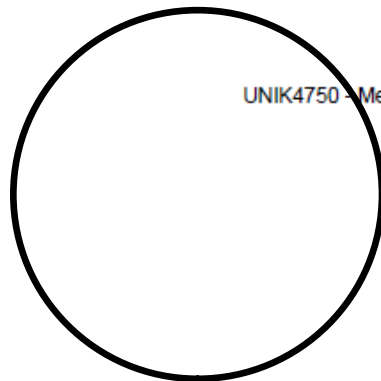
$0.64 \cdot 60 = 38.4$

12:45 cont.

14:00 guest lecture

Establish Application Goals for Security & Privacy

- Discuss with your neighbours the security and privacy goal for :
- Billing (1/hour)
 - Security, Privacy Goal: (s,p) - Range [0...100]
- Fire alarm
 - Security, Privacy Goal: (s,p) - Range [0...100]
- Home Control (1/hour)
 - Security, Privacy Goal: (s,p) - Range [0...100]



UNIK4750 - Measurable Security

Goal:
“basis of discussion”
- why?