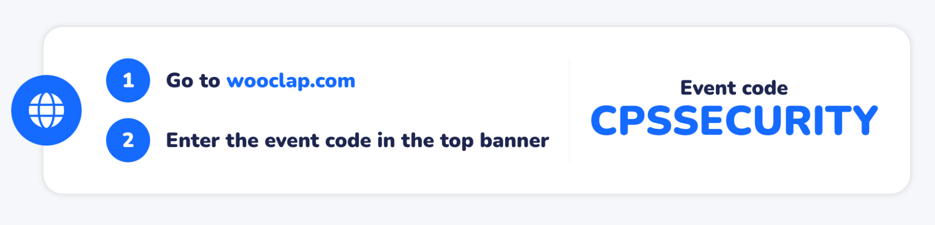
CE/CZ4055 Cyber Physical System Security

Secure Communication in CPS

Anupam Chattopadhyay
CCDS, NTU



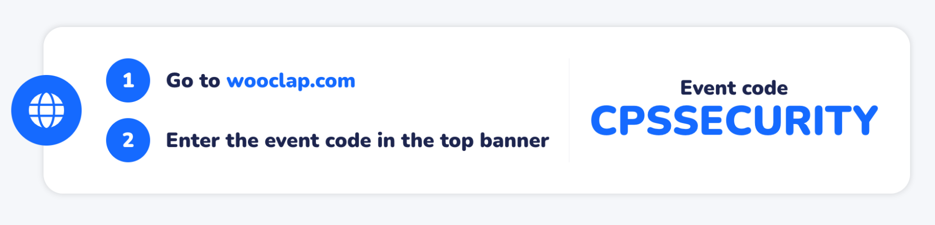
1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

Contents

- *Secure Communication in SCADA*
- Secure Communication in Bluetooth
- Secure Communication in Wi-Fi
- Discussion



1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

Supervisory Control And Data Acquisition (SCADA)

- Real time industrial process control systems to monitor and control remote or local industrial equipment

- Part of Critical Infrastructure (e.g., Water, Electricity)

- Risk of large-scale attacks!

Nicholson et al.' 2012. SCADA security in the light of Cyber-Warfare. Computers & Security, vol. 31, 2012.

SCADA Systems

- 1960: mainframe computer supervision
- 1970: general purpose operating systems
- 1990: off the shelf computing
- Highly distributed with central control
- Field devices control local operations

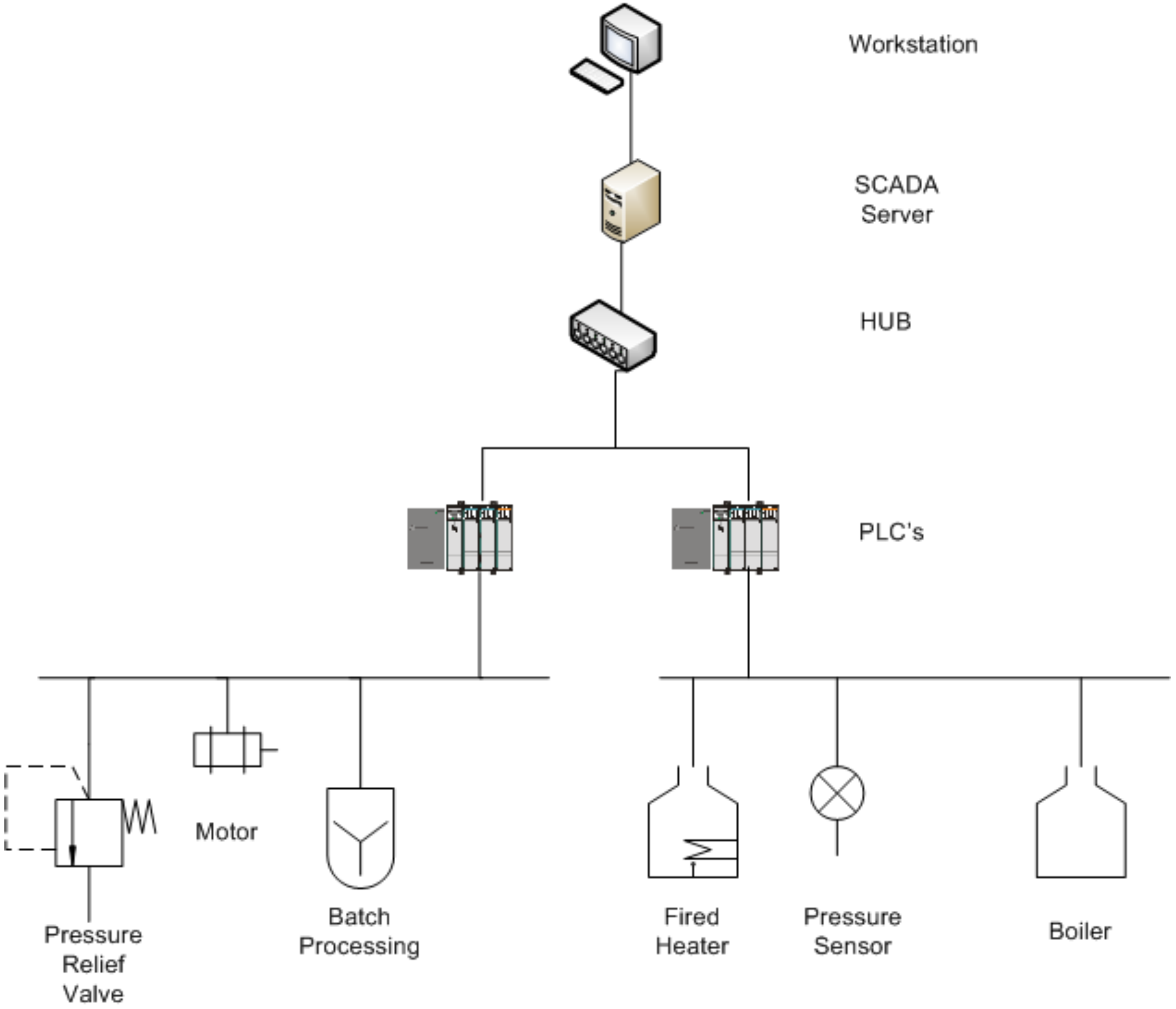
SCADA Incidents

- 1986: Chernobyl Soviet Union
  - 56 direct death, 4000 related cancer death
- 1999: Whatcom Creeks Washington US pipeline rupture
  - Spilling 237,000 gallons of gasoline that ignited, 3 human life and all aquatic life
- 2003: North East Blackout of US and Canada
  - Affected 55 million people, 11 death
- 2011: Fukushima Daiichi nuclear disaster Japan
  - Loss of human lives, cancer, psychological distress

SCADA Components

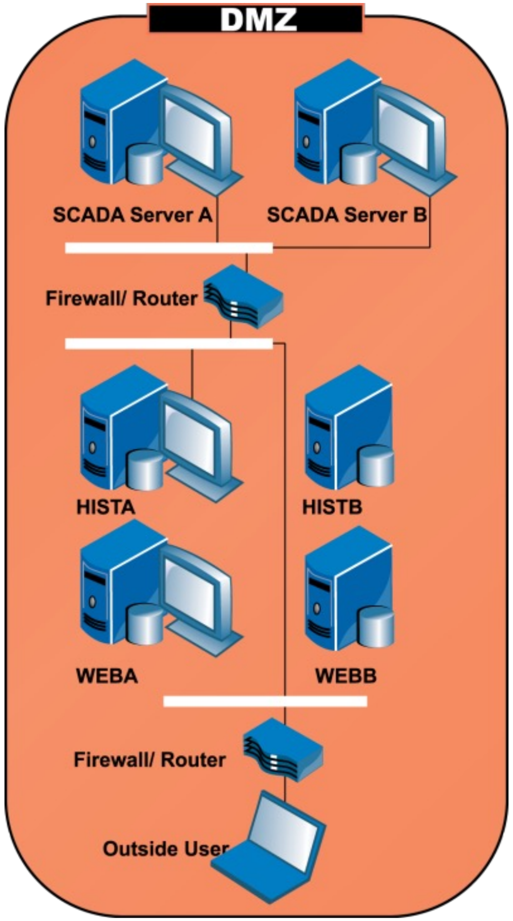
- Corporate network segment
  - Typical IT network
- SCADA network segment
  - Servers and workstations to interact with field devices
  - Human-machine interfaces
  - Operators
  - Software validation
- Field devices segment
  - Programmable Logic Controllers (PLC)
  - Remote Terminal Units (RTU)
  - Intelligent Electronic Devices (IED)

SCADA Hierarchy

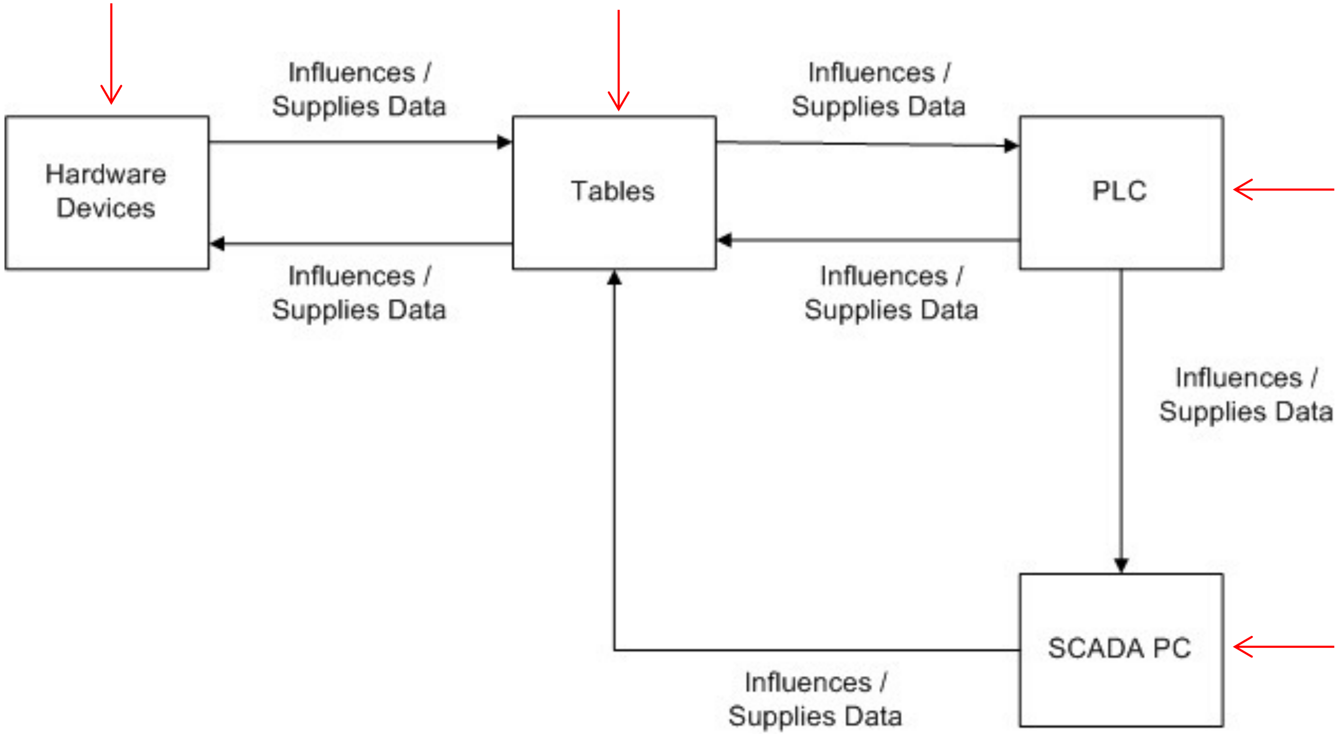


SCADA Security

- Perimeter Protection
  - Firewall, VPN
  - Host Intrusion Detection System (IDS)
  - Host Antivirus (AV)
  - Demilitarized Zone (DMZ)
- Interior Security
  - Firewall, IDS, VPN, AV
  - Host IDS, Host AV
  - Network Access Control (NAC)
  - Scanning
- Monitoring
- Management



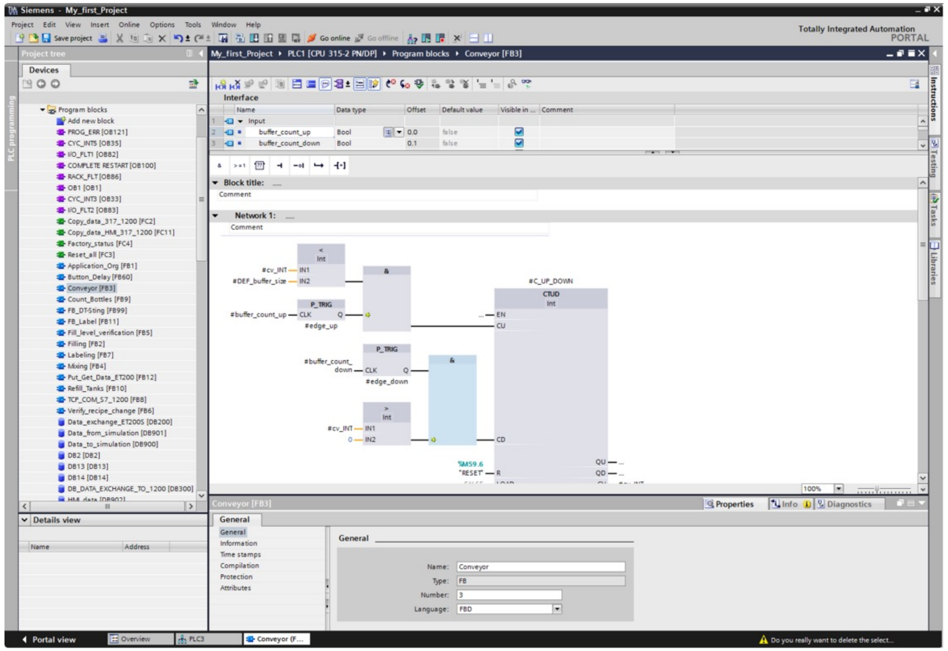
SCADA and PLC Security


Hardware Devices
Tables
PLC
SCADA PC
Influences / Supplies Data
Influences / Supplies Data
Influences / Supplies Data
Influences / Supplies Data
Influences / Supplies Data
Influences / Supplies Data

SCADA System Control Flow

SCADA and PLC Security

- **Stuxnet attack** (2010): First well-publicized attack targeting PLCs.
- Microsoft Windows (zero-day attack) → Siemens Simatic Step7 software → Control, Monitor, Reconfigure PLCs.



My_first_Project ▸ PLC1 [CPU 315-2 PN/DP] ▸ Program blocks ▸ Conveyor [FB3]

Program blocks
Add new block
PROG_ERR [OB121]
CYC_INT5 [OB35]
I/O_FLT1 [OB82]
COMPLETE RESTART [OB100]
RACK_FLT [OB86]
OB1 [OB1]
CYC_INT3 [OB33]
I/O_FLT2 [OB83]
Copy_data_317_1200 [FC2]
Copy_data_HMI_317_1200 [FC11]
Factory_status [FC4]
Reset_all [FC3]
Application_Org [FB1]
Button_Delay [FB60]
Conveyor [FB3]
Count_Bottles [FB9]
FB_DT-Sting [FB99]
FB_Label [FB11]
Fill_level_verification [FB5]
Filling [FB2]
Labeling [FB7]
Mixing [FB4]
Put_Get_Data_ET200 [FB12]
Refill_Tanks [FB10]
TCP_COM_S7_1200 [FB8]
Verify_recipe_change [FB6]
Data_exchange_ET200S [DB200]
Data_from_simulation [DB901]
Data_to_simulation [DB900]
DB2 [DB2]
DB13 [DB13]
DB14 [DB14]
DB_DATA_EXCHANGE_TO_1200 [DB300]
HMI_data [DB902]

Details view

Name	Address

Interface

	Name	Data type	Offset	Default value	Visible in ...	Comment
1	Input					
2	buffer_count_up	Bool	0.0	false	☑	
3	buffer_count_down	Bool	0.1	false	☑	

Block title: ......
Comment

Network 1: ......
Comment

Conveyor [FB3]

General
General
Information
Time stamps
Compilation
Protection
Attributes

General

Name: Conveyor
Type: FB
Number: 3
Language: FBD

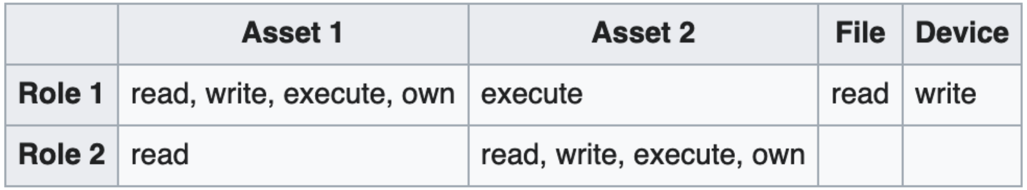
Do you really want to delete the select...

Attack Severity Analysis: Severity Chart

Severity	Effects in PLC	Effects in SCADA
A	PLC Code will not perform the desired tasks	Will not allow for remote operation of the process
B	Serious hindrance to the process	The process could experience intermittent process failure
C	Adversely effects PLC code performance. A minimal cost effect to the project, but a “quick fix” is possible	Data shown on the SCADA screen is most likely false
D	Effects the credibility of the system, but the PLC code is operable	Incorrect data could be randomly reported, cause a lack of confidence in the system

Restricted Communication

- Access Control Matrix



	Asset 1	Asset 2	File	Device
Role 1	read, write, execute, own	execute	read	write
Role 2	read	read, write, execute, own		

- Physically enforced through one-way diode or data diode

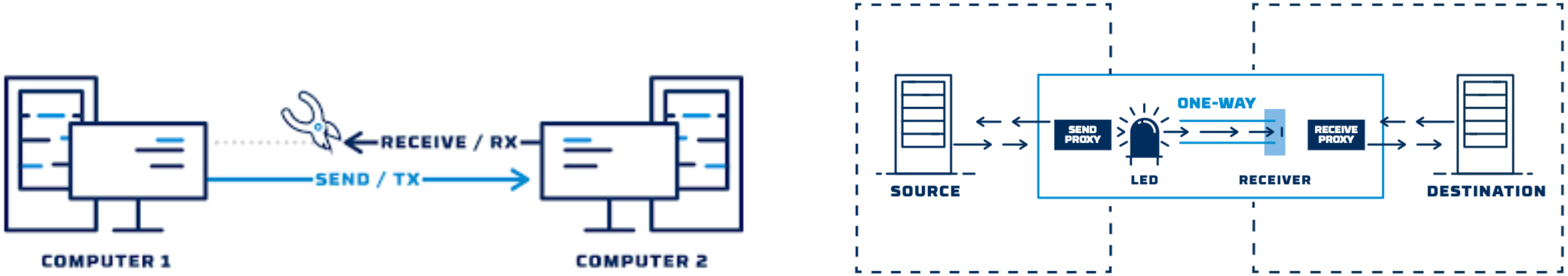
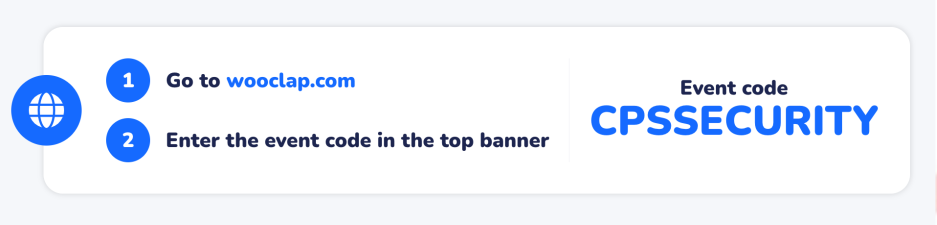


Image: Owl Cyber Defense

Contents

- Secure Communication in SCADA
- *Secure Communication in Bluetooth*
- Secure Communication in Wi-Fi
- Discussion



1 Go to wooclap.com

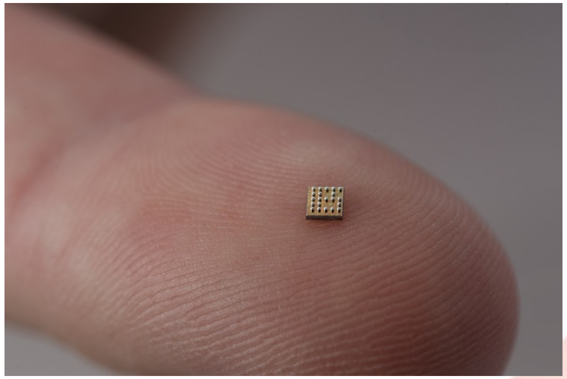
2 Enter the event code in the top banner

Event code

CPSSECURITY

Bluetooth

- Developed by a group called Bluetooth Special Interest Group (SIG), formed in May 1998
  - Founding members were Ericsson, Nokia, Intel, IBM and Toshiba
- Bluetooth connects different wireless devises, like laptops, mobile phones, PDAs, refrigerators etc.
- Bit rates up to 1 Mbps
- Low cost ($1-$2) and small size

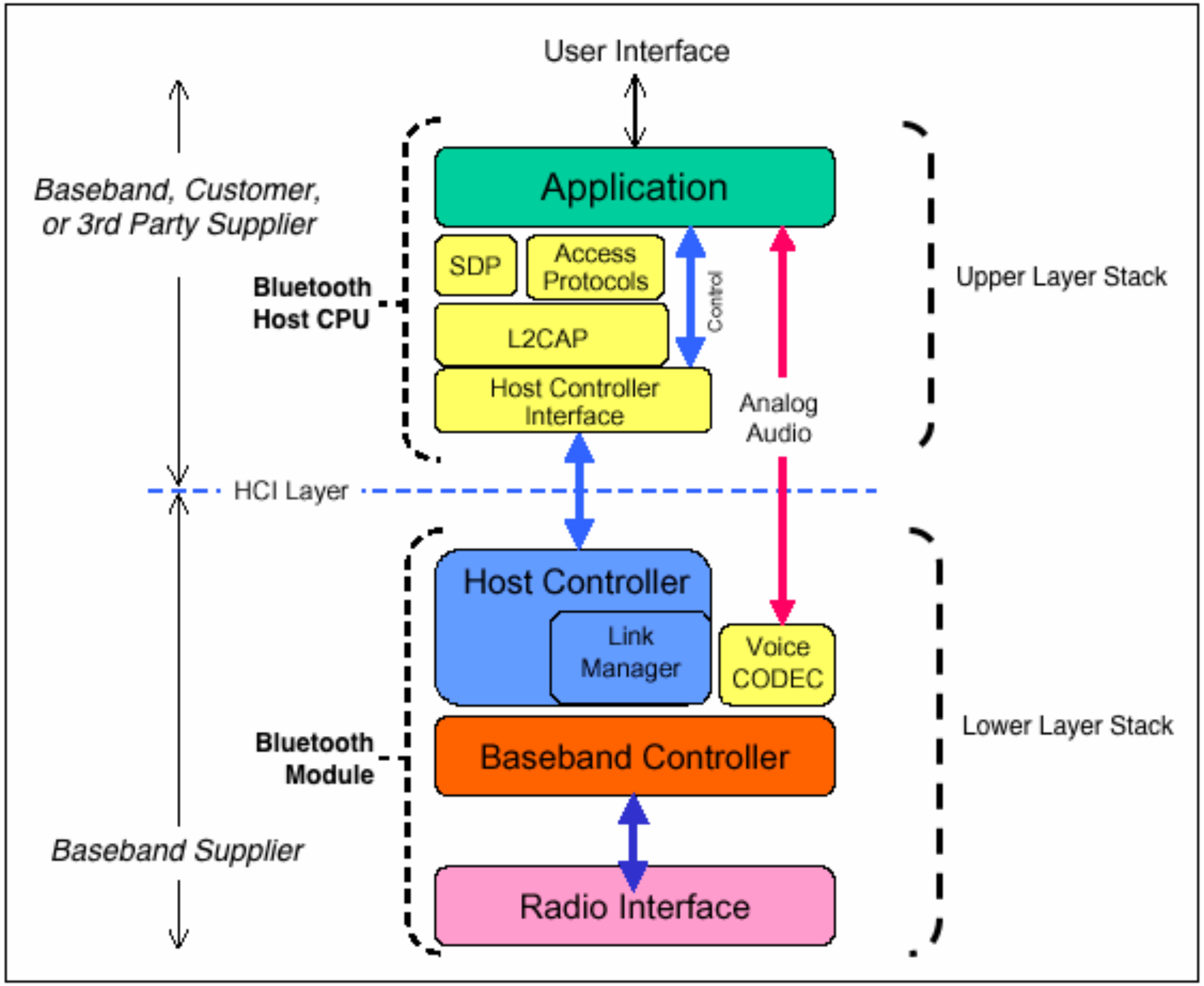


5 mm^2 Bluetooth chip designed by Swatch group
Contains 5M transistors.

Bluetooth components

- **Radio unit**
  - Technologies: Time-Division Duplex (TDD) and Frequency Hopping Spread Spectrum (FHSS)
- **Baseband unit**
  - Voice to data conversion, packet segmentation, master/slave communication, identification of parties, *control authorization*
- **Link Management Protocol (LMP)**
  - Set up connections and implement *security features like key exchanges and encryption*
- **Logical Link Control and Adaptation Protocol (L2CAP)**
  - Multiplexing, packer segmentation/reassembly, QoS
- **Service Discovery Protocol (SDP)**
  - Queries a Bluetooth device and checks what services it supports

Bluetooth protocol Architecture



Bluetooth security features

- The Bluetooth specification include security features at the link level
- Supports authorization, authentication and encryption
- Based on a *secret link key that is shared by a pair of devices*
- Link key generated by a *pairing procedure* when two devices communicate for the first time

Security modes of Bluetooth (1)

- Security mode 1
  - No security, for testing only. Allows other Bluetooth devices initiate connections with it, PUSH messages
- Security mode 2
  - A device does not initiate security procedures before establishment of the link between the devices at the L2CAP level
  - Security policies can flexibly impose different trust levels: *authentication*, *authorization* and *encryption*

Security modes of Bluetooth (2)

- Security mode 3
  - Security at the Baseband level
  - Security manager imposes security policies
  - LMP makes encryption and key exchanges

Key Management (1)

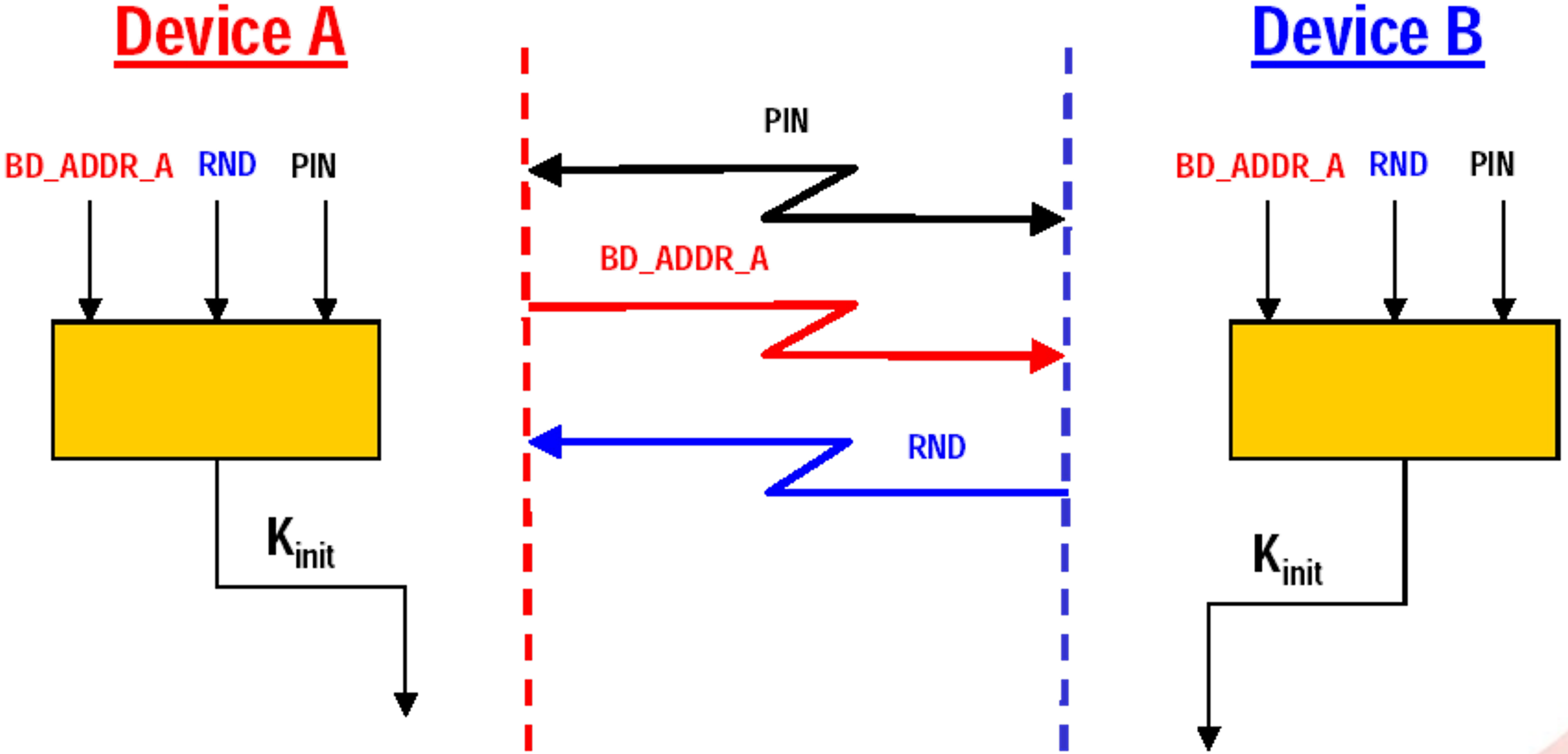
- Link keys
  - All keys are 128-bit random numbers and are either temporary or semi-permanent
  - Unit key K_A , unique long-term private key of a device
  - Combination key K_{AB} derived from units A and B. Generated for each pair of devices
  - Master key K_{master}, used when master device wants to transmit to several devices at once
  - Initialization key K_{init}, used in the initialization process.

Key Management (2)

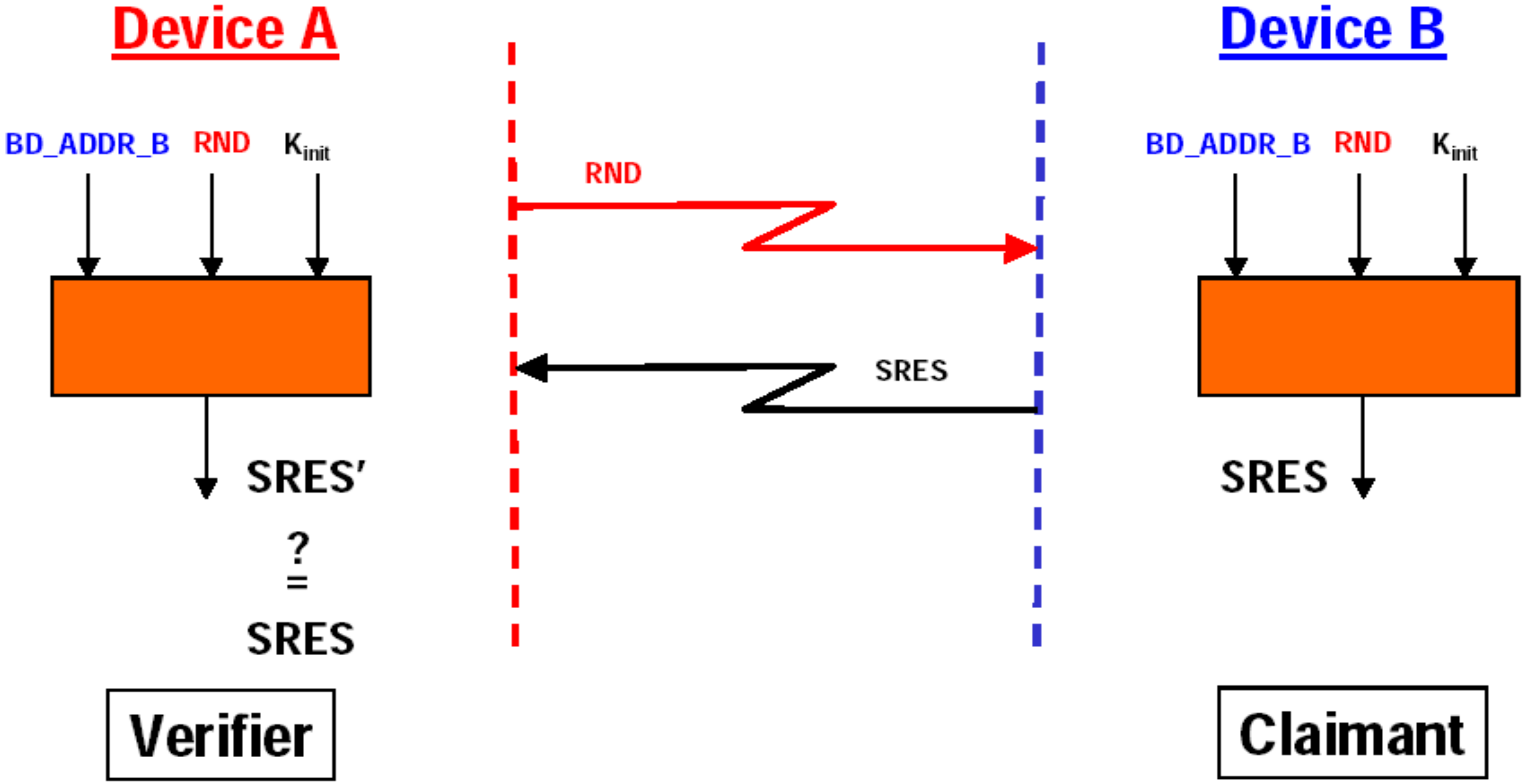
- Encryption key
  - Derived from the current link key. Each time encryption is needed the encryption key will be automatically changed
  - Separated from authentication key

- PIN Code
  - Fixed or selected by the user
  - Usually 4 digits, can be 8 to 128 bits
  - Shared secret

Establishment of Initialization Key *(Pairing)*

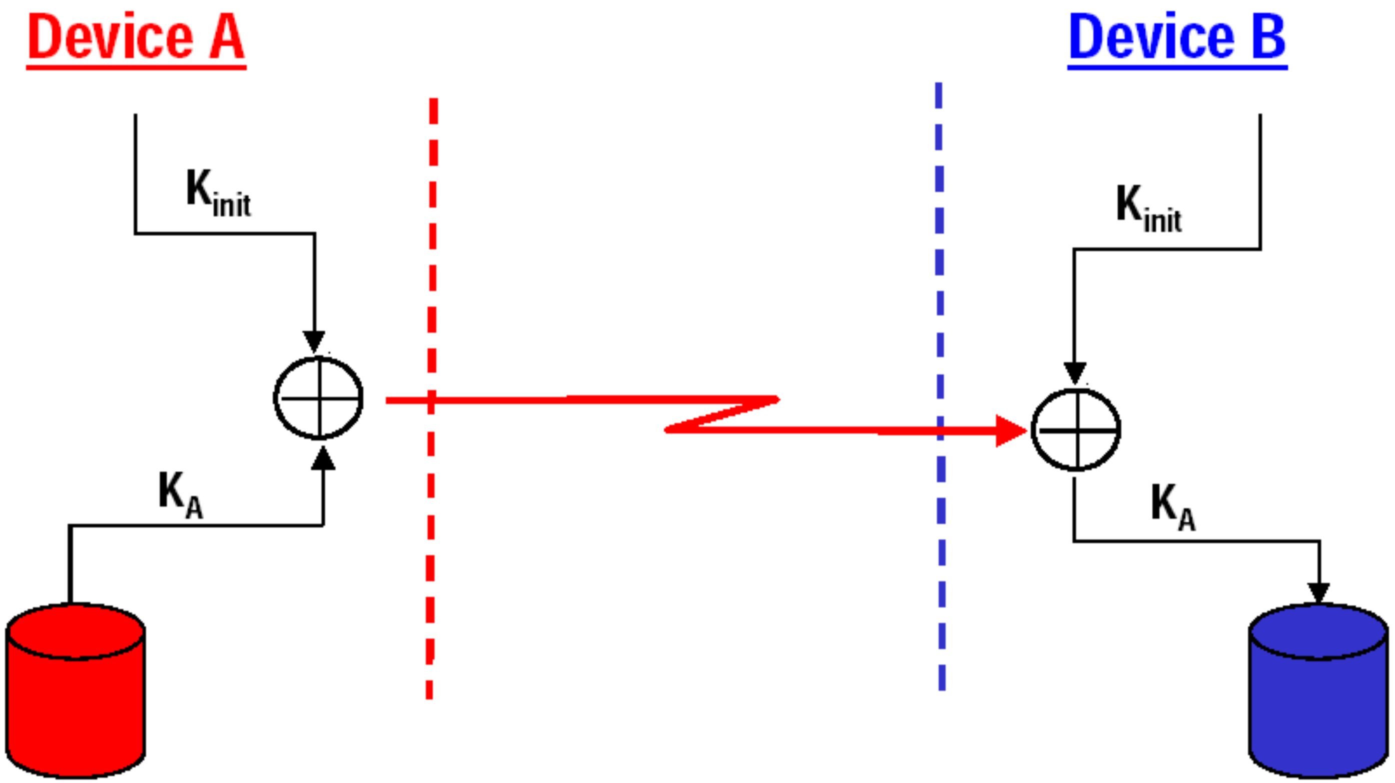


Verification of Initialization Key *(Pairing)*



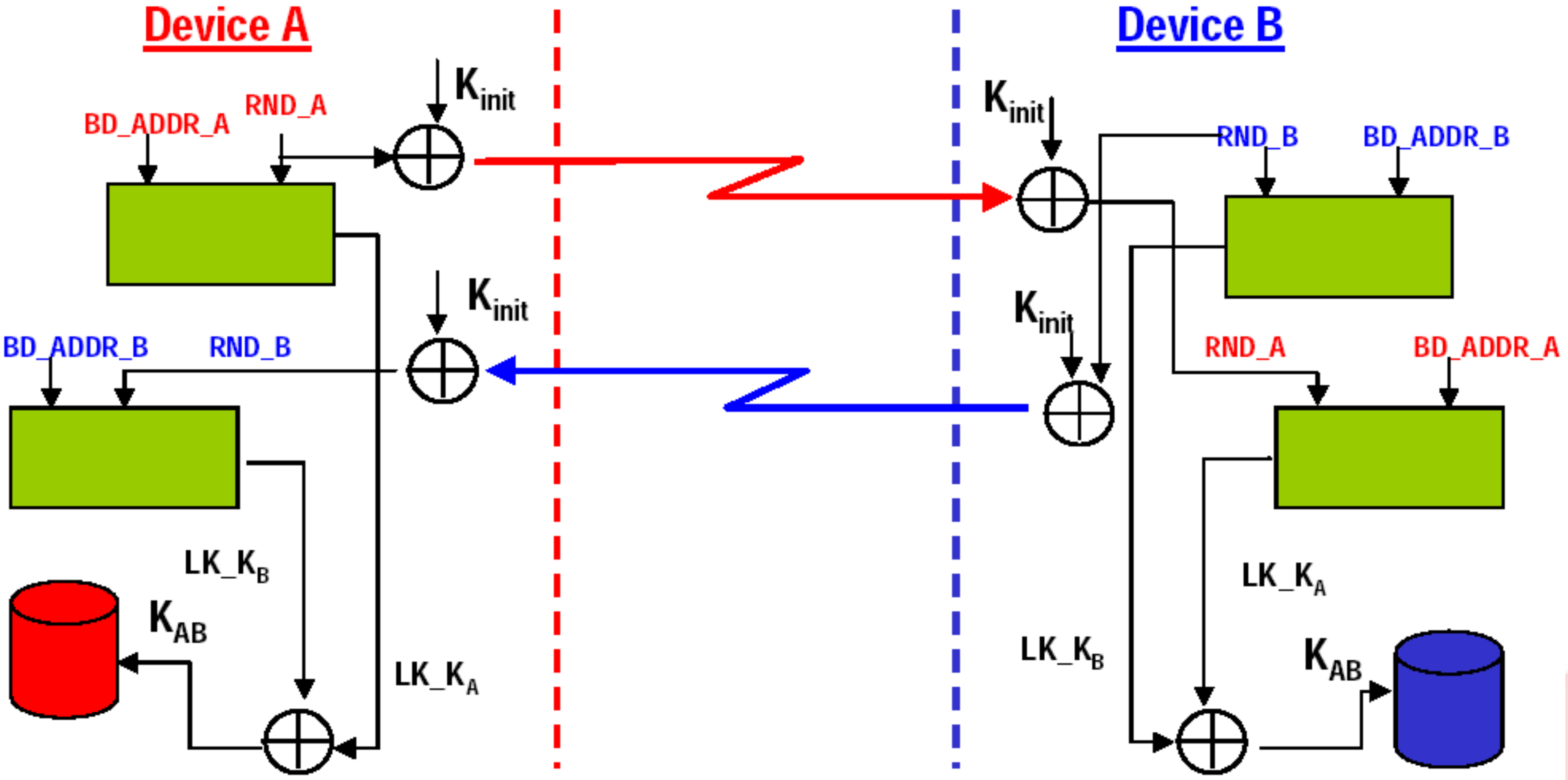
Establishment of Link Key (1) *(Pairing)*

- Link key of devices A and B = unit key K_A of device A



Establishment of Link Key (2) *(Pairing)*

- Link key of devices A and B = combination key K_{AB}



Authentication and Encryption

- Authentication by issuing a **challenge** to another device

- The other device replies to challenge with a message based on the **challenge**, the **Device address** and the **shared link key.**

- The device that issued the challenge verifies the response and authenticates if the response is equals to its own calculations.

- Encryption is based on the stream cipher

Bluetooth security weaknesses (1)

- **PIN weakness**
  - Initial authentication is based on a PIN that can be anywhere between 8-128 bits
  - If poorly chosen can be easy to guess
- **Impersonation**
  - Stealing the Unit Key
  - Only the device is authenticated, not the user
- **Replay attacks**
  - A hacker can record Bluetooth then replay the whole transmission e.g., repeat payment

Bluetooth security weaknesses (2)

- **Man in the middle**
  - Bluetooth authentication is not based on public key certificates. It is possible to play man in the middle

- **Location attack**
  - A Bluetooth device has (globally) a unique identification number; therefore it is possible to identify and locate user's position

- **Denial-of-Service attack**
  - Jamming the whole frequency band, takes lot of energy
  - Identify the ‘hopping sequence’, used for avoiding interference

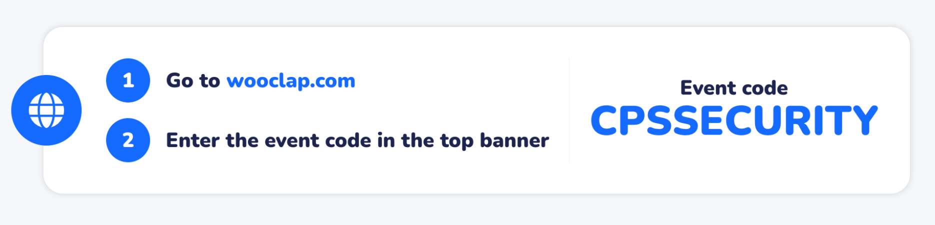
Image Courtesy: Ubertooth

How to avoid being attacked

- Pairing in secure place
- Long PIN numbers are strongly encouraged
- Avoid using unit keys. Use combination keys
- Respond only to known devices

Contents

- Secure Communication in SCADA
- Secure Communication in Bluetooth
- *Secure Communication in Wi-Fi*
- Discussion



1 Go to wooclap.com

2 Enter the event code in the top banner

Event code

CPSSECURITY

IEEE 802.11 Wireless LAN

- IEEE 802: a committee responsible for LANs

- IEEE 802.11: responsible for developing wireless protocols
  - Many standards

- The Wi-Fi alliance: became popular with 802.11b
  - Wi-Fi Protected Access (WPA, WPA2)

IEEE 802.11# Wireless Security

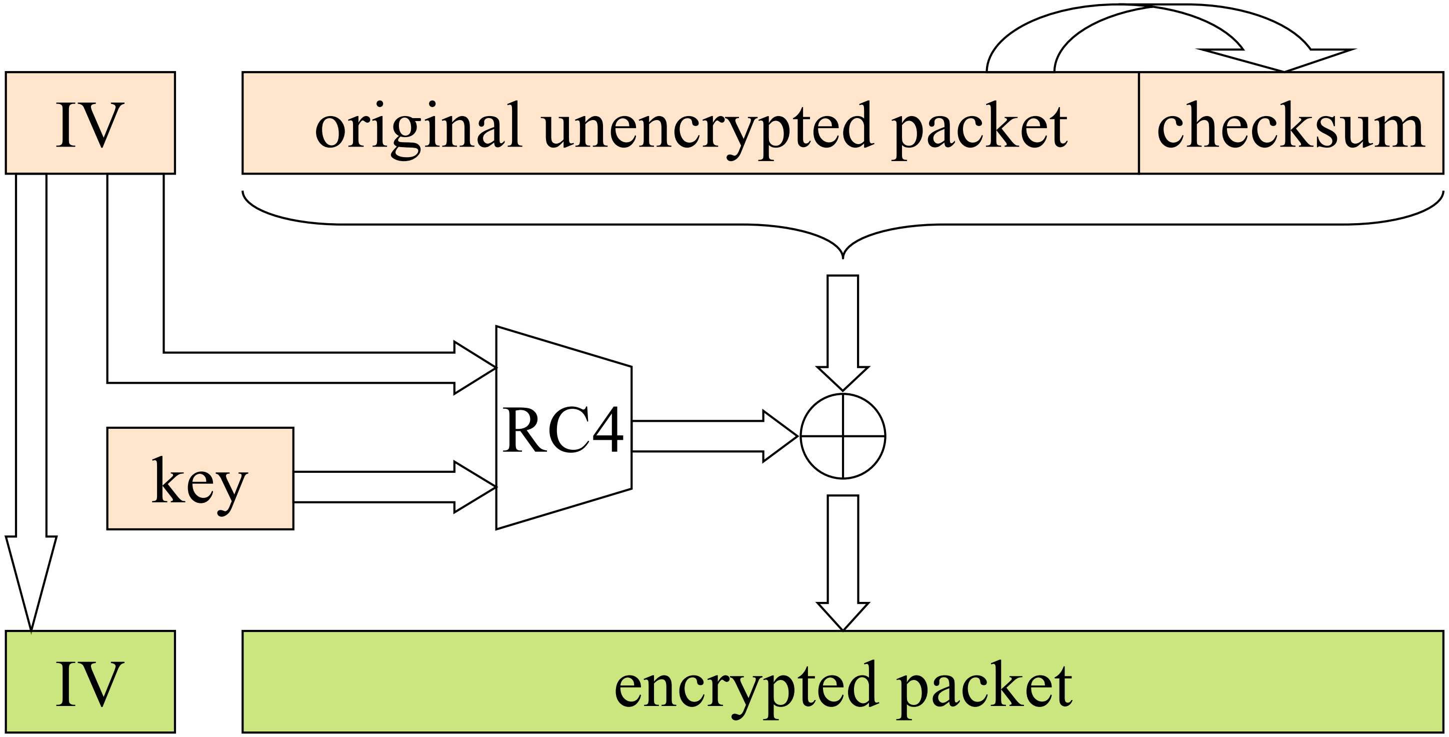
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- WPA2
- WPA3 (announced in 2018)

WEP - Wired Equivalent Privacy

- The original native security mechanism for WLAN provides security through 802.11 network

- Used to protect wireless communication from eavesdropping (*confidentiality*)
- Prevent unauthorized access to a wireless network (*authenticity*)
- Prevent tampering with transmitted messages (*integrity*)

How WEP works



WEP Flaws and Vulnerabilities

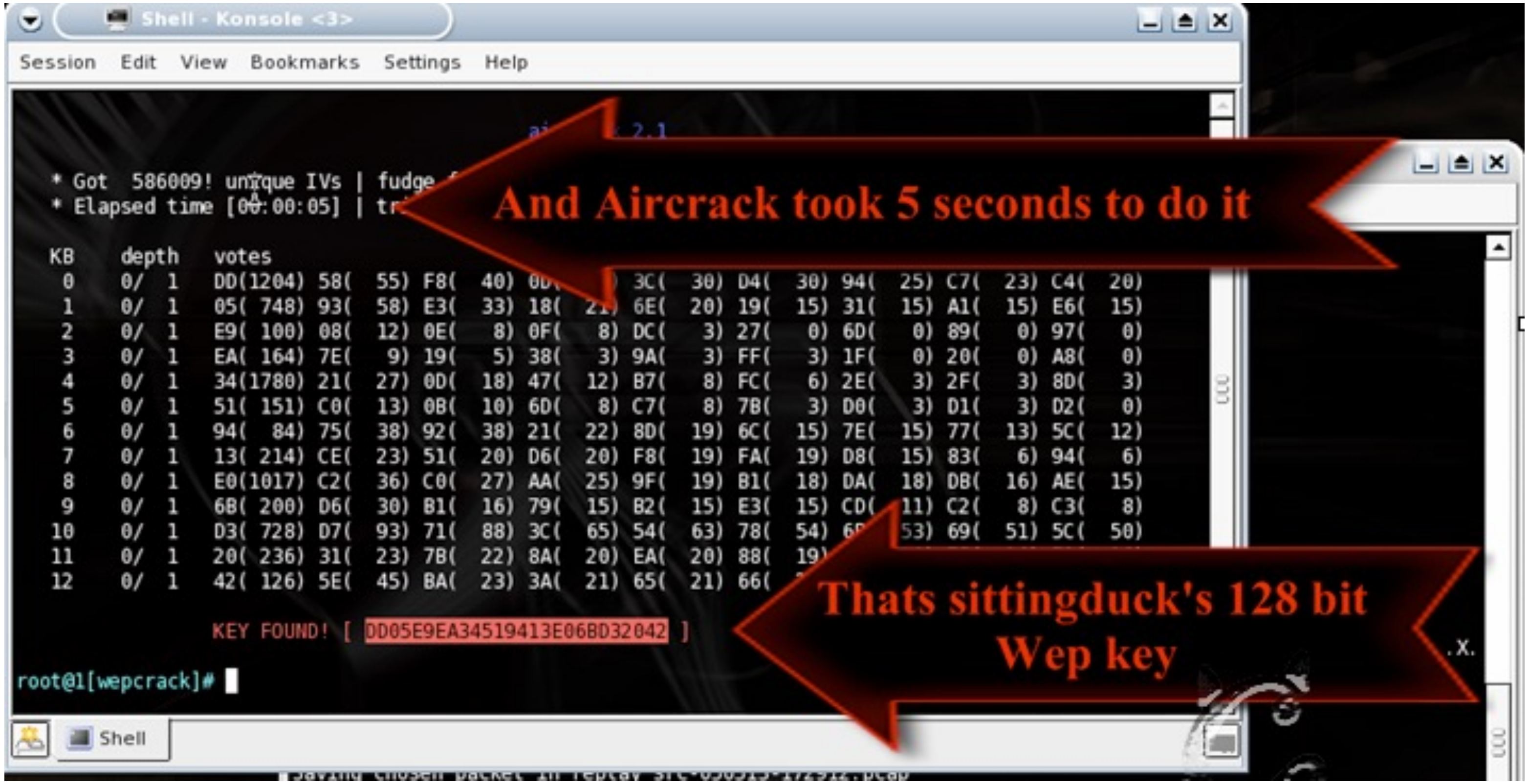
- Weak keys:
  - ✓ It allows an attacker to discover the default key being used by the Access Point and client stations
  - ✓ This enables an attacker to decrypt all messages being sent over the encrypted channel

- IV (initialization vector) reuse and small size:
  - ✓ On a busy network, the IV is reused. In that scenario, if the default key has not been changed, the original message can be retrieved relatively easily

Attacks on WEP

- WEP encrypted networks can be cracked in 10 minutes
- Goal is to collect enough IVs to be able to crack the key
- Injecting packets generates IVs
- Attacks on RC4 (deprecated)

WEP Cracking Example



Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
Shell
And Aircrack took 5 seconds to do it
Thats sittingduck's 128 bit Wep key

```
                                     ai        2.1

  * Got  586009! unique IVs | fudge f
  * Elapsed time [00:00:05] | tr

  KB    depth   votes
   0    0/  1   DD(1204) 58(  55) F8(  40) 0D(       3C(  30) D4(  30) 94(  25) C7(  23) C4(  20)
   1    0/  1   05( 748) 93(  58) E3(  33) 18(  21) 6E(  20) 19(  15) 31(  15) A1(  15) E6(  15)
   2    0/  1   E9( 100) 08(  12) 0E(   8) 0F(   8) DC(   3) 27(   0) 6D(   0) 89(   0) 97(   0)
   3    0/  1   EA( 164) 7E(   9) 19(   5) 38(   3) 9A(   3) FF(   3) 1F(   0) 20(   0) A8(   0)
   4    0/  1   34(1780) 21(  27) 0D(  18) 47(  12) B7(   8) FC(   6) 2E(   3) 2F(   3) 8D(   3)
   5    0/  1   51( 151) C0(  13) 0B(  10) 6D(   8) C7(   8) 7B(   3) D0(   3) D1(   3) D2(   0)
   6    0/  1   94(  84) 75(  38) 92(  38) 21(  22) 8D(  19) 6C(  15) 7E(  15) 77(  13) 5C(  12)
   7    0/  1   13( 214) CE(  23) 51(  20) D6(  20) F8(  19) FA(  19) D8(  15) 83(   6) 94(   6)
   8    0/  1   E0(1017) C2(  36) C0(  27) AA(  25) 9F(  19) B1(  18) DA(  18) DB(  16) AE(  15)
   9    0/  1   6B( 200) D6(  30) B1(  16) 79(  15) B2(  15) E3(  15) CD(  11) C2(   8) C3(   8)
  10    0/  1   D3( 728) D7(  93) 71(  88) 3C(  65) 54(  63) 78(  54) 6    53) 69(  51) 5C(  50)
  11    0/  1   20( 236) 31(  23) 7B(  22) 8A(  20) EA(  20) 88(  19)
  12    0/  1   42( 126) 5E(  45) BA(  23) 3A(  21) 65(  21) 66(

                KEY FOUND! [ DD05E9EA34519413E06BD32042 ]

root@1[wepcrack]#
```

WPA - WI-FI Protected Access

- New technique in 2002
- Replacement of security flaws of WEP
- Improved data encryption, strong user authentication
- Because of many attacks related to static key, WPA minimize shared secret key in accordance with the frame transmission
- Use the RC4 algorithm in a proper way and provide fast transfer of the data before someone can decrypt the data

WPA2 - WI-FI Protected Access 2

- Based on the IEEE 802.i standard
- 2 versions: Personal, Enterprise

- The primary enhancement over WPA is the use of the Advanced Encryption Standard (AES) algorithm
- The Personal mode uses a Pre-shared Key (PSK) and does not require a separate authentication of users
- The enterprise mode requires the users to be separately authenticated by using the Extensible Authentication Protocol (EAP)
    - Based on Certificates (instead of passwords)

WEP vs WPA vs WPA2

	WEP	WPA	WPA2
ENCRYPTION	RC4	RC4	AES
KEY ROTATION	NONE	Dynamic Session Keys	Dynamic Session Keys
KEY DISTRIBUTION	Manually typed into each device	Automatic distribution available	Automatic distribution available
AUTHENTICATION	Uses WEP key as Authentication	Can use 802.1x and EAP	Can use 802.1x and EAP

WPA3

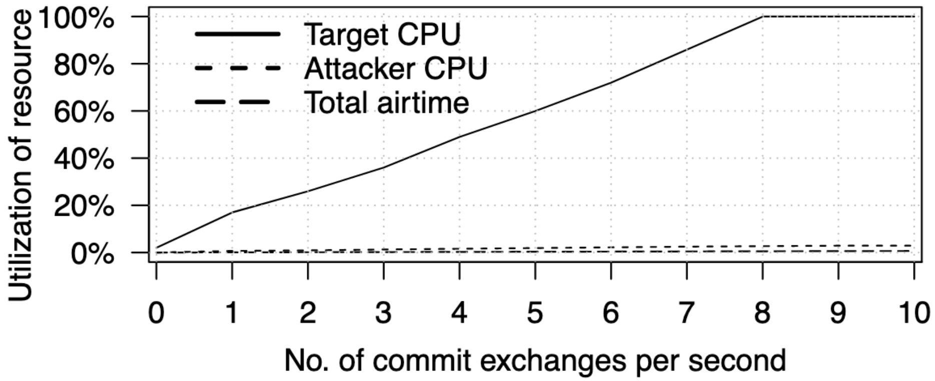
- Replaces pre-shared keys with Simultaneous Authentication of Equals (SAE) method, also called Dragonfly handshake
  - A type of password-authenticated key exchange
- Frequent update of keys guarantee even a breach cannot be leveraged to know the past secrets (*forward secrecy*)
- Dragonfly handshake
  - Internally calls ECDH key agreement protocol
  - Dragonblood attack[1]

[1] *https://wpa3.mathyvanhoef.com/*

Dragonblood Attacks

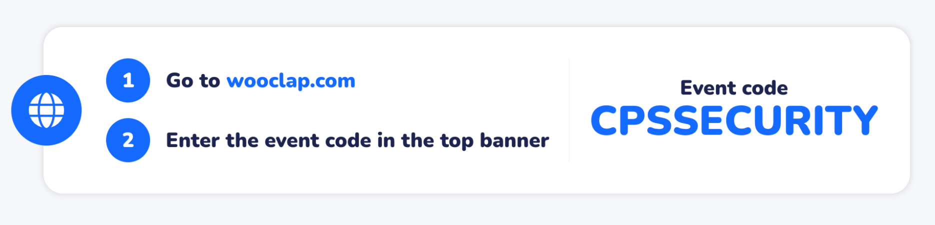
- Downgrade attack (when supporting both WPA2 and WPA3)

- Denial-of-Service Attack
  - Dragonfly has high runtime overhead due to its *hash* operations, and is further appended with dummy operations to protect against timing leakages
  - This is exploited to inject false commit frames to the Access Point, which keeps the AP too busy to address other clients



Contents

- Secure Communication in SCADA
- Secure Communication in Bluetooth
- Secure Communication in Wi-Fi
- ➔ *Discussion*



1 Go to wooclap.com

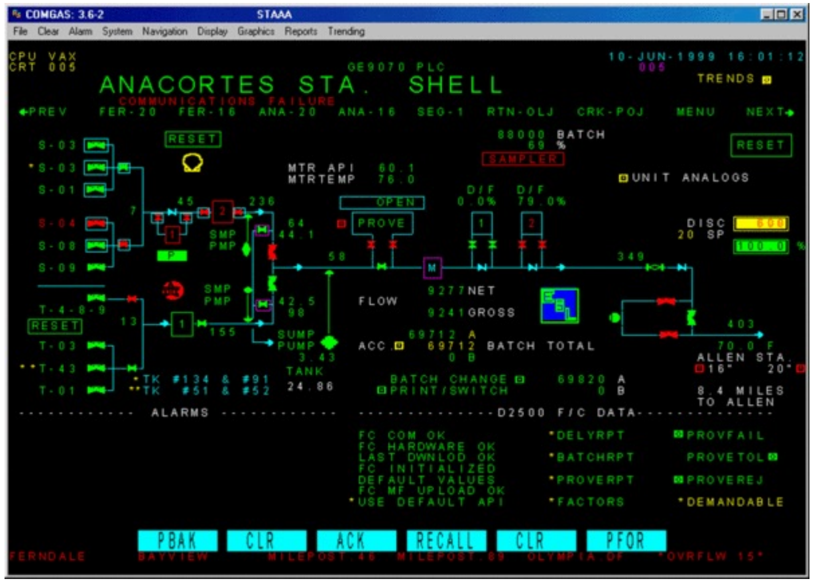
2 Enter the event code in the top banner

Event code

CPSSECURITY

What did we learn?

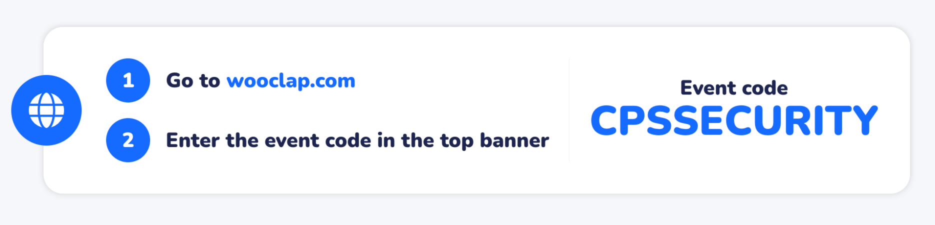
- **Usage of SCADA and PLC**
  - Threats, Protections
  - PLC vulnerability
  - One-way Diode



FC COM OK
FC HARDWARE OK
LAST DWNLOD OK
FC INITIALIZED
DEFAULT VALUES
FC MF UPLOAD OK
*USE DEFAULT API

- **Bluetooth/Wi-Fi Communication**
  - Security protocols
  - Vulnerabilities

The End



1 Go to wooclap.com

2 Enter the event code in the top banner

Event code

CPSSECURITY

NANYANG TECHNOLOGICAL UNIVERSITY