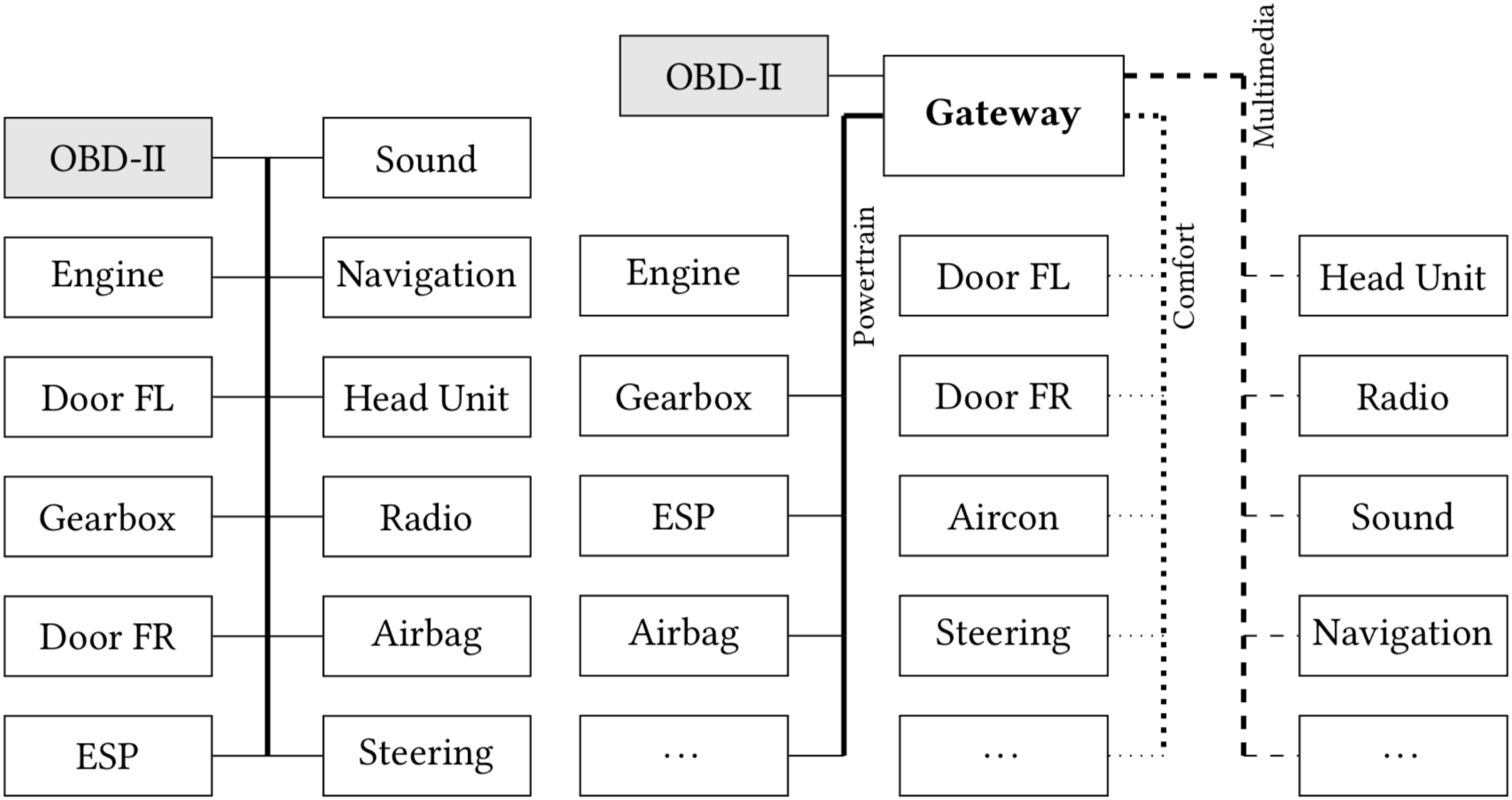
# Scission

Paper By: Marcel Kneib and Christopher Huth

Presented By: Aaron Zhang

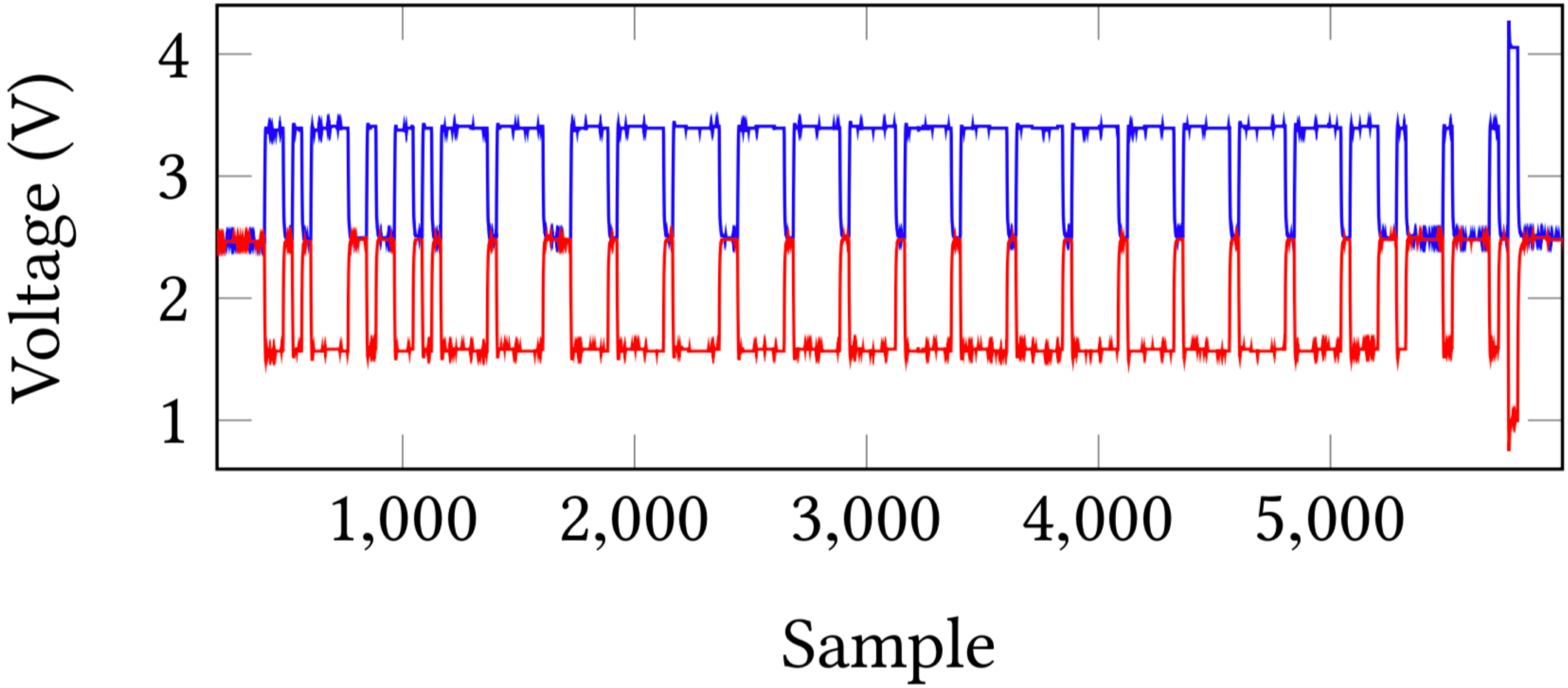
# Outline

- **Background Information**
- How Scission Works
- Implementation
  - Fingerprinting ECUs
  - Detecting Compromised ECUs
- Conclusion



(a) Simple

(b) Complex

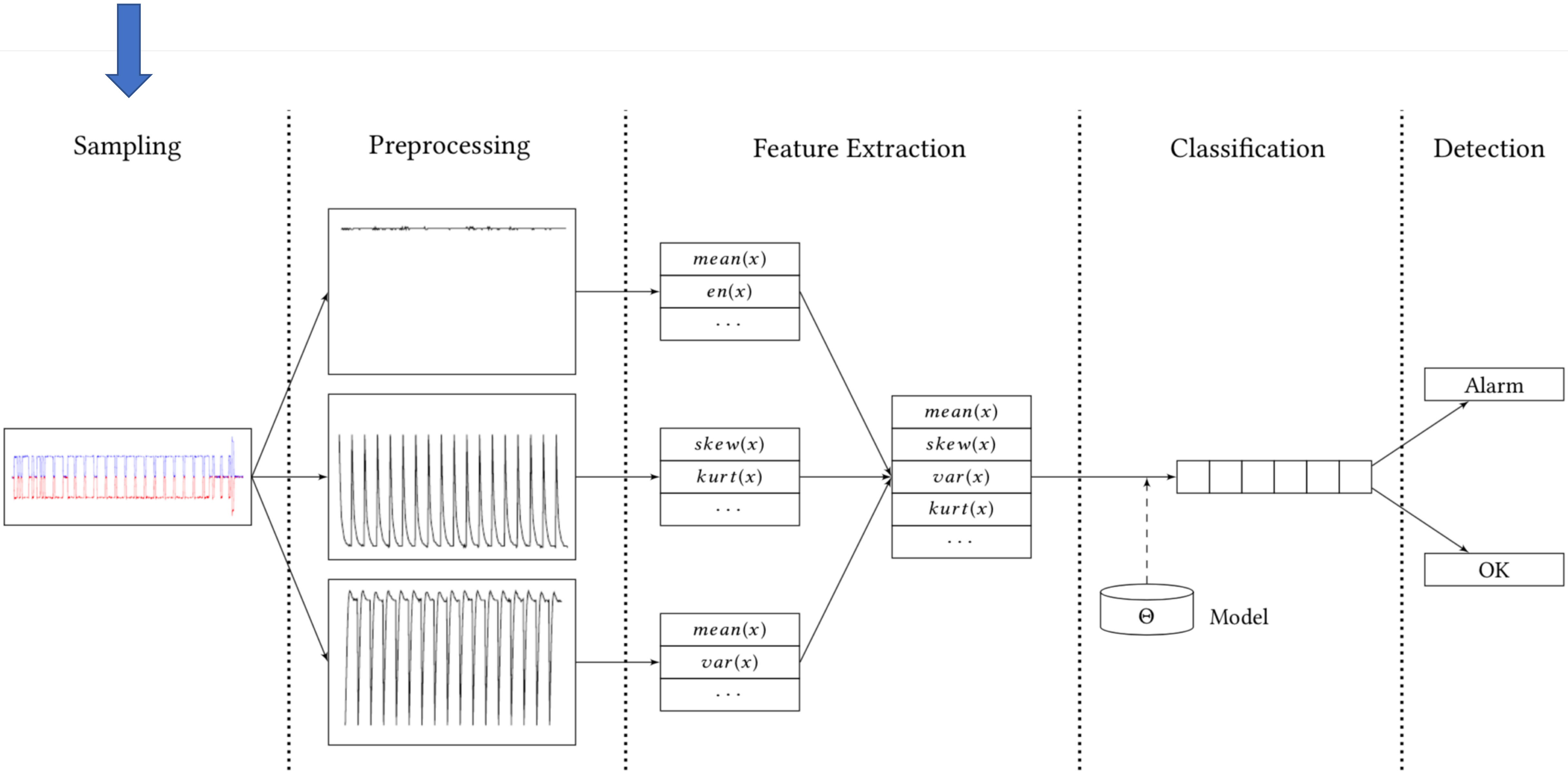

Voltage (V)
4
3
2
1
1,000
2,000
3,000
4,000
5,000
Sample

# Possible Attacks

- Compromised ECUs
  - Changing of a preexisting ECU
- Unmonitored ECUs
  - A read only ECU changes into a writing ECU
- Additional ECUs
  - Connecting a compromised ECU to the network

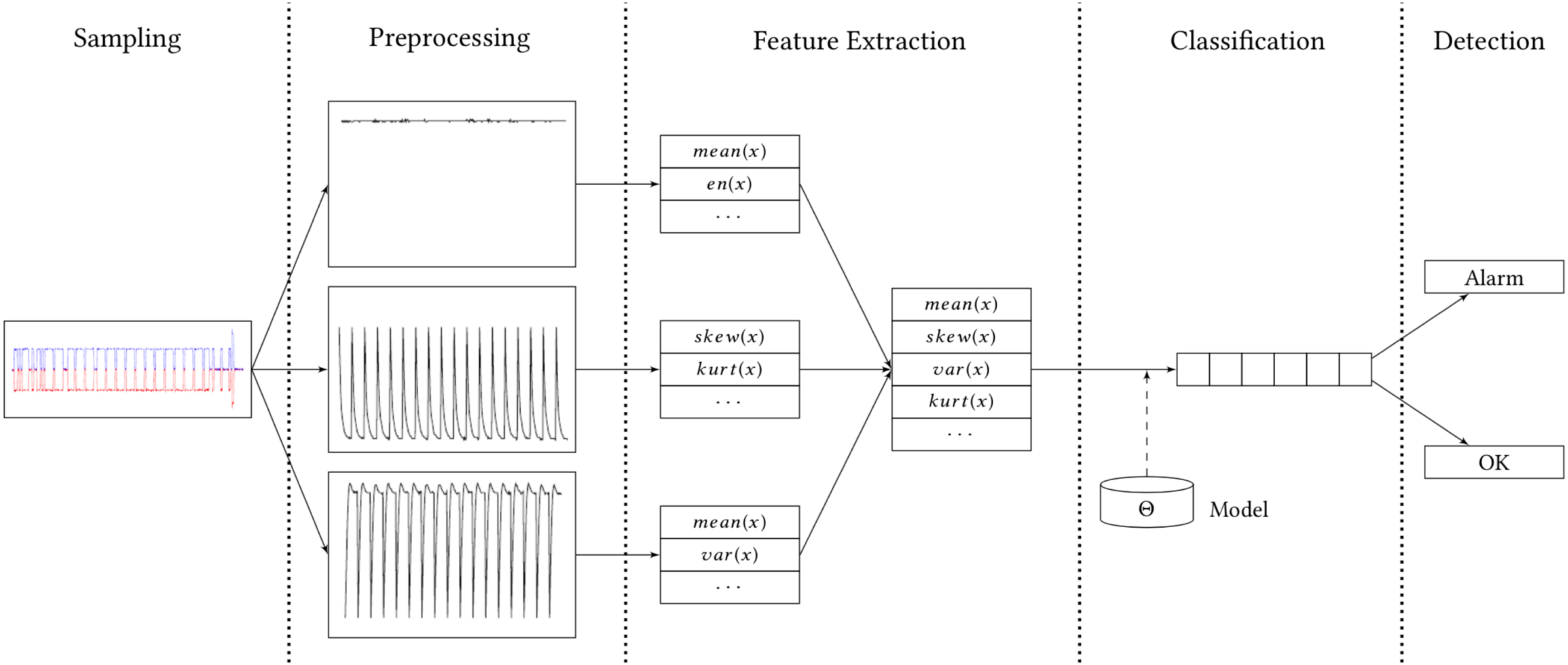
# Outline

- Background Information
- **How Scission Works**
- Implementation
  - Fingerprinting ECUs
  - Detecting Compromised ECUs
- Conclusion


Sampling
Preprocessing
Feature Extraction
Classification
Detection
$mean(x)$
$en(x)$
...
$skew(x)$
$kurt(x)$
...
$mean(x)$
$var(x)$
...
$mean(x)$
$skew(x)$
$var(x)$
$kurt(x)$
...
Θ
Model
Alarm
OK

# Difference in Signal Data

- Variations in Supply Voltage
- Variations in Grounding
- Variations in Resistors, Termination and Cables.
- Imperfection in Bus Topology causing reflections



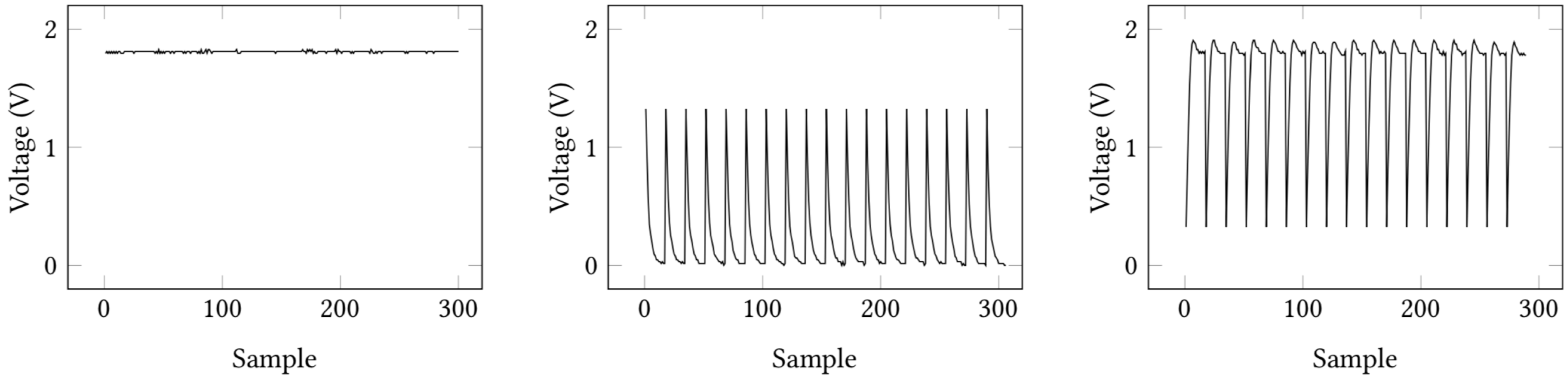
Sampling

Preprocessing

Feature Extraction

Classification

Detection



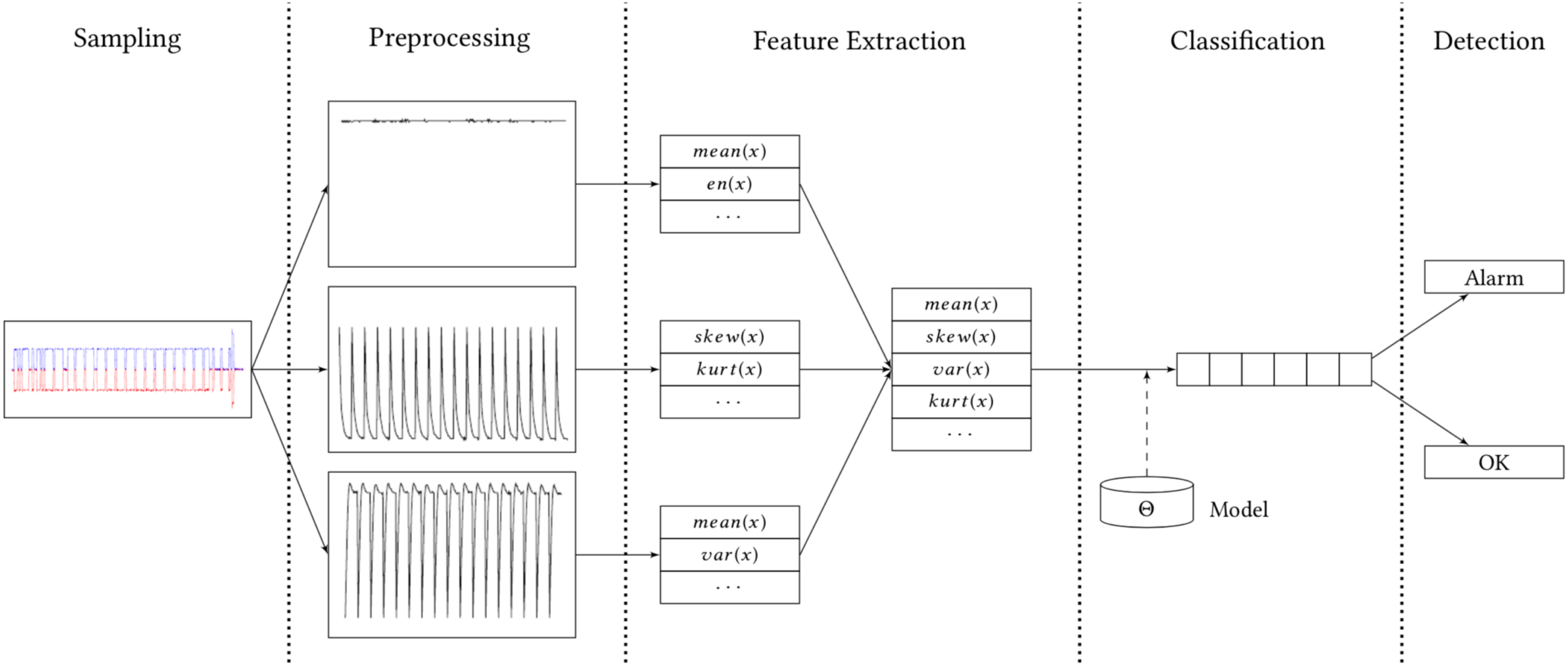
**(a) Group 00 containing 17 symbols**

**(b) Group 01 containing 18 symbols**

**(c) Group 10 containing 17 symbols**

# Signal Bit Groups

- Dominant Bit Rising G10
- Dominant Bit not Rising G00
- Recessive Bit Falling G01
- Dominant Bit following another Dominant bit(G11) are ignored since they will always be value 0



Sampling

Preprocessing

Feature Extraction

$mean(x)$

$en(x)$

$\dots$

$skew(x)$

$kurt(x)$

$\dots$

$mean(x)$

$var(x)$

$\dots$

$mean(x)$

$skew(x)$

$var(x)$

$kurt(x)$

$\dots$

Classification

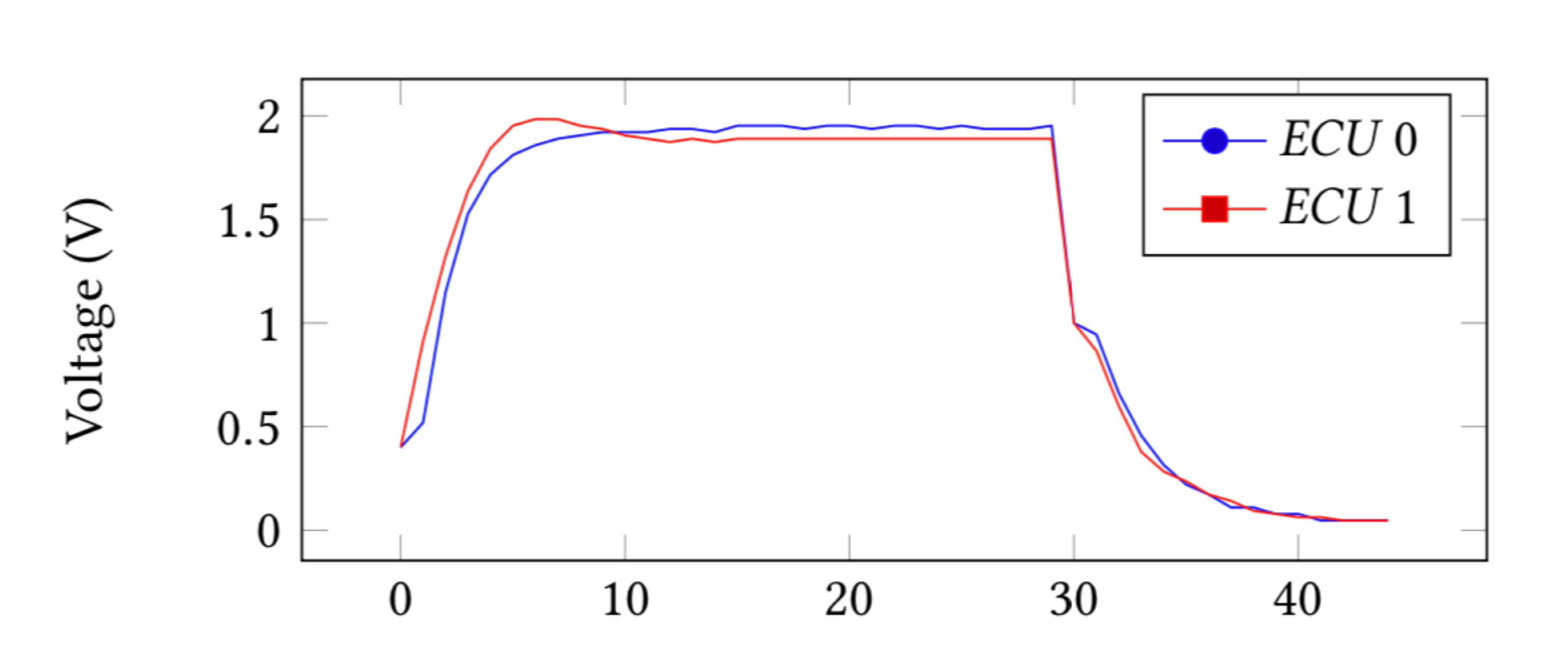
$\Theta$

Model

Detection

Alarm

OK



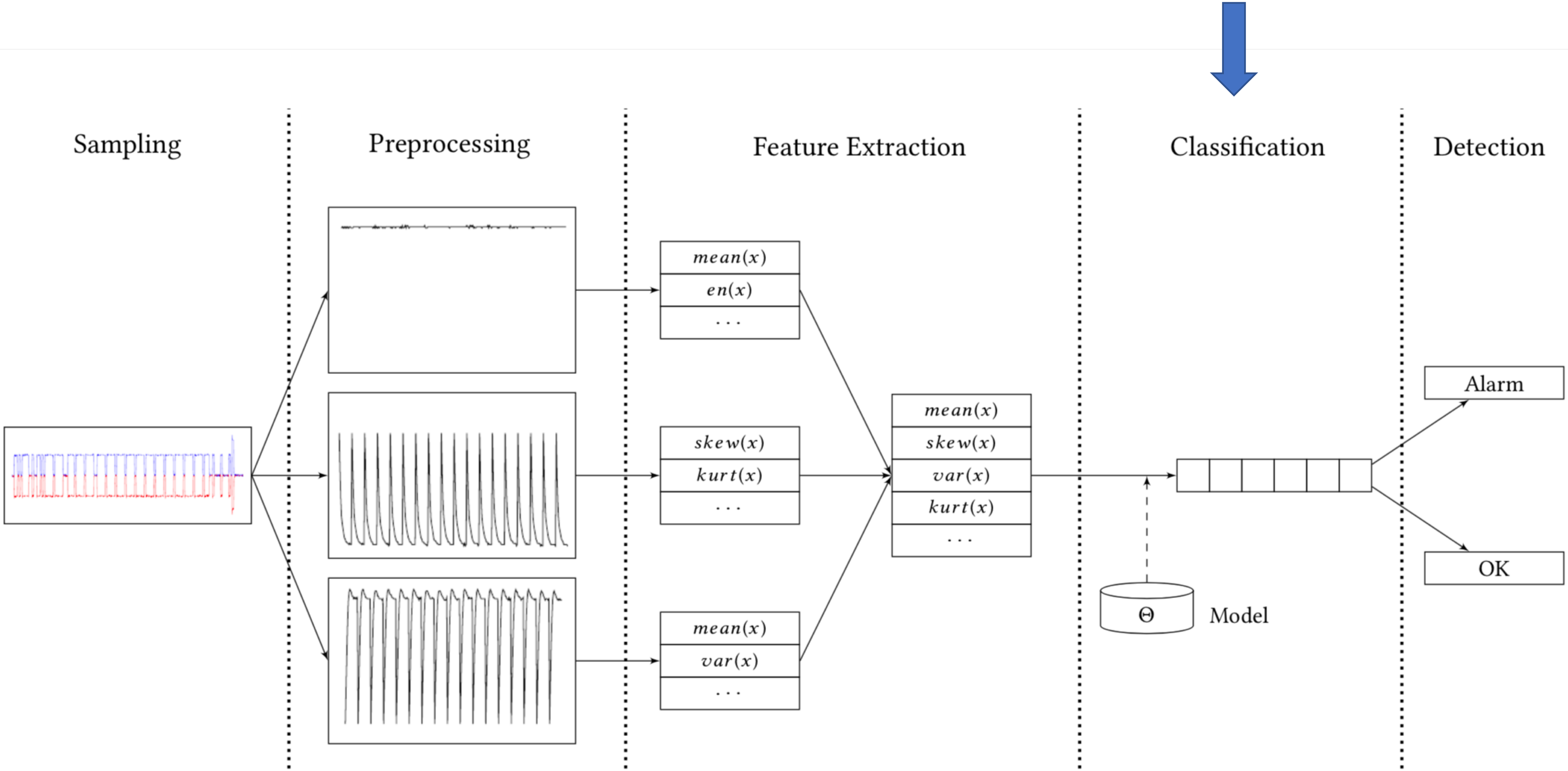
Mean(ECU 0) = 1.286

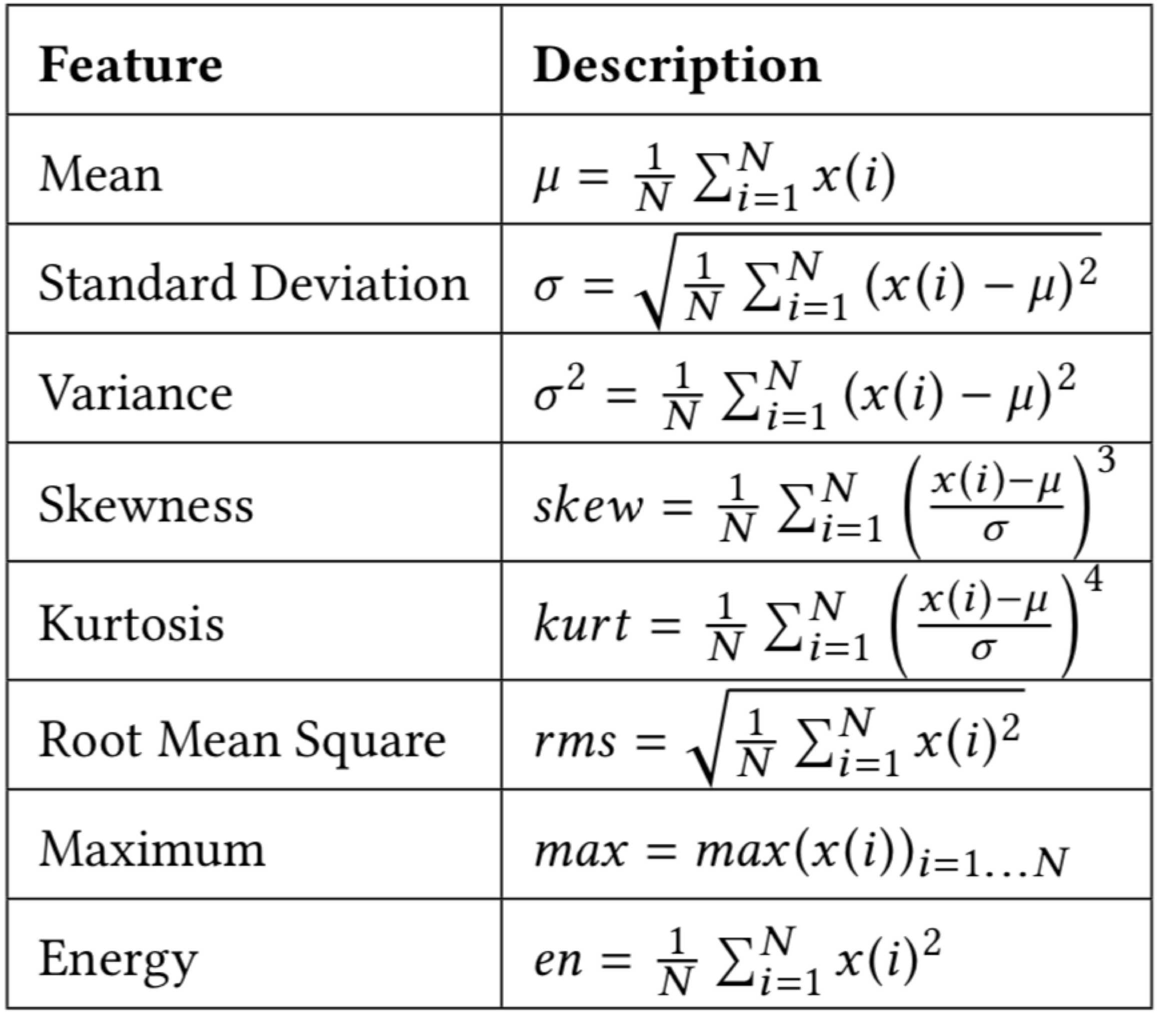
Mean(ECU 1) = 1.285

# Differences Between ECUs

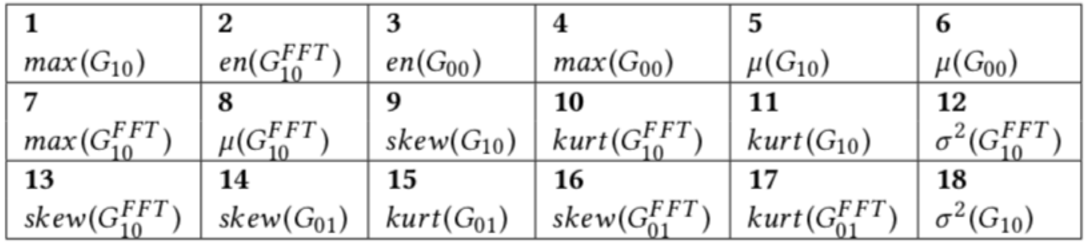
- ECU 0
- Mean(G10) = 1.623
- Mean(G00) = 1.947
- Mean(G01) = 0.289

- ECU 1
- Mean(G10) = 1.691
- Mean(G00) = 1.89
- Mean(G01) = 0.275


Sampling
Preprocessing
Feature Extraction
Classification
Detection
$mean(x)$
$en(x)$
...
$skew(x)$
$kurt(x)$
...
$mean(x)$
$var(x)$
...
$mean(x)$
$skew(x)$
$var(x)$
$kurt(x)$
...
Θ
Model
Alarm
OK



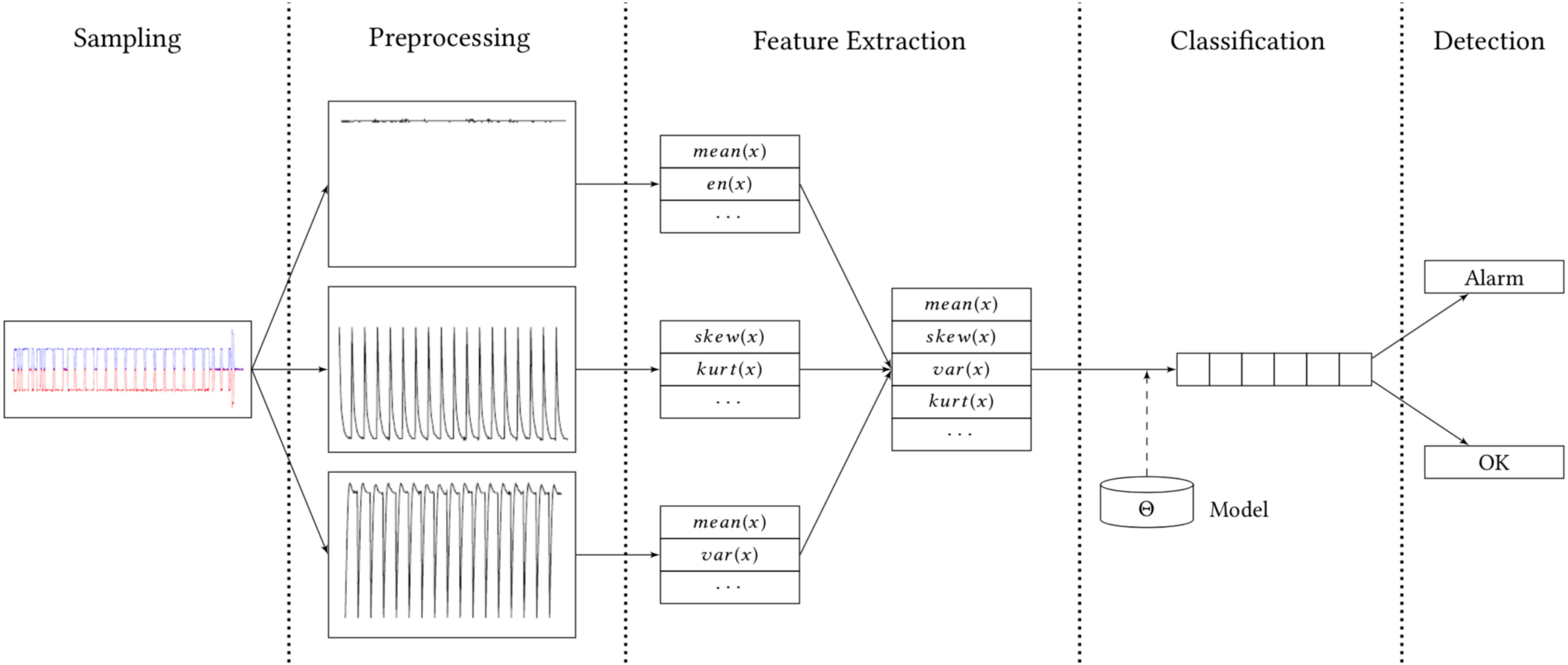
| **Feature** | **Description** |
|---|---|
| Mean | $\mu = \frac{1}{N}\sum_{i=1}^{N} x(i)$ |
| Standard Deviation | $\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x(i)-\mu)^2}$ |
| Variance | $\sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(x(i)-\mu)^2$ |
| Skewness | $skew = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{x(i)-\mu}{\sigma}\right)^3$ |
| Kurtosis | $kurt = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{x(i)-\mu}{\sigma}\right)^4$ |
| Root Mean Square | $rms = \sqrt{\frac{1}{N}\sum_{i=1}^{N} x(i)^2}$ |
| Maximum | $max = max(x(i))_{i=1\ldots N}$ |
| Energy | $en = \frac{1}{N}\sum_{i=1}^{N} x(i)^2$ |



| | | | | | |
|---|---|---|---|---|---|
| **1**<br>$max(G_{10})$ | **2**<br>$en(G_{10}^{FFT})$ | **3**<br>$en(G_{00})$ | **4**<br>$max(G_{00})$ | **5**<br>$\mu(G_{10})$ | **6**<br>$\mu(G_{00})$ |
| **7**<br>$max(G_{10}^{FFT})$ | **8**<br>$\mu(G_{10}^{FFT})$ | **9**<br>$skew(G_{10})$ | **10**<br>$kurt(G_{10}^{FFT})$ | **11**<br>$kurt(G_{10})$ | **12**<br>$\sigma^2(G_{10}^{FFT})$ |
| **13**<br>$skew(G_{10}^{FFT})$ | **14**<br>$skew(G_{01})$ | **15**<br>$kurt(G_{01})$ | **16**<br>$skew(G_{01}^{FFT})$ | **17**<br>$kurt(G_{01}^{FFT})$ | **18**<br>$\sigma^2(G_{10})$ |

# Deployment and Lifecycle

- The identification and fingerprinting should only be implemented in a perfect environment such as the factory in which a car is made.
- A key is assigned to each ECU.


Sampling
Preprocessing
Feature Extraction
Classification
Detection
$mean(x)$
$en(x)$
...
$skew(x)$
$kurt(x)$
...
$mean(x)$
$var(x)$
...
$mean(x)$
$skew(x)$
$var(x)$
$kurt(x)$
...
$\Theta$
Model
Alarm
OK

## Detecting Compromised ECUs

- The receiving ECU compares the received message to the possible messages, if it is not similar, an attack is assumed.

## Detecting Unmonitored ECUs

- Frames are labelled as suspicious if no ECU can be assigned to the received message. If the amount of suspicious frames exceed an arbitrary number, an attack is assumed.

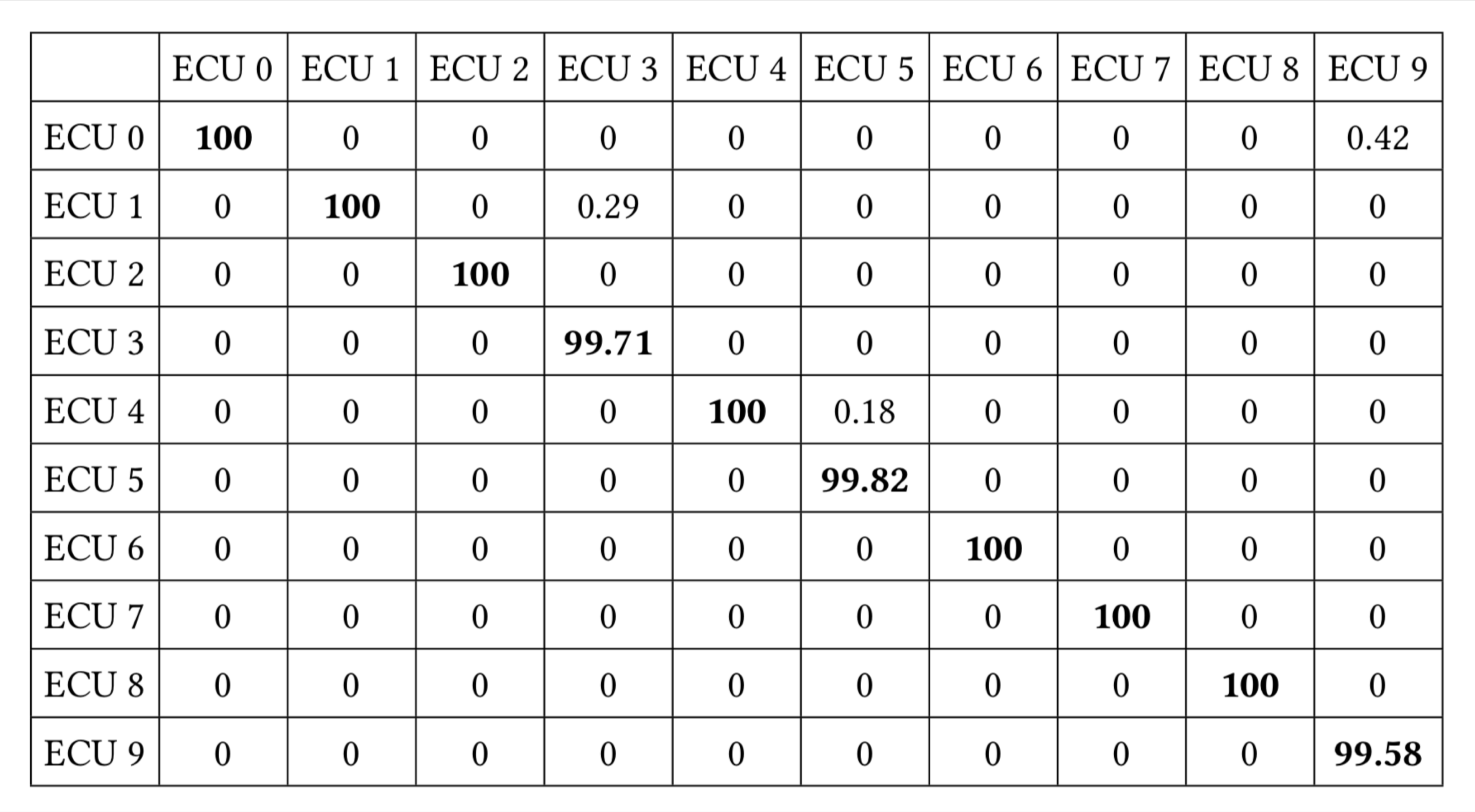
## Detecting Additional ECUs

- Similar to Unmonitored, but the entirety of the CAN Network can change based on an addition ECU, increasing the total amount of suspicious frames.

# Outline

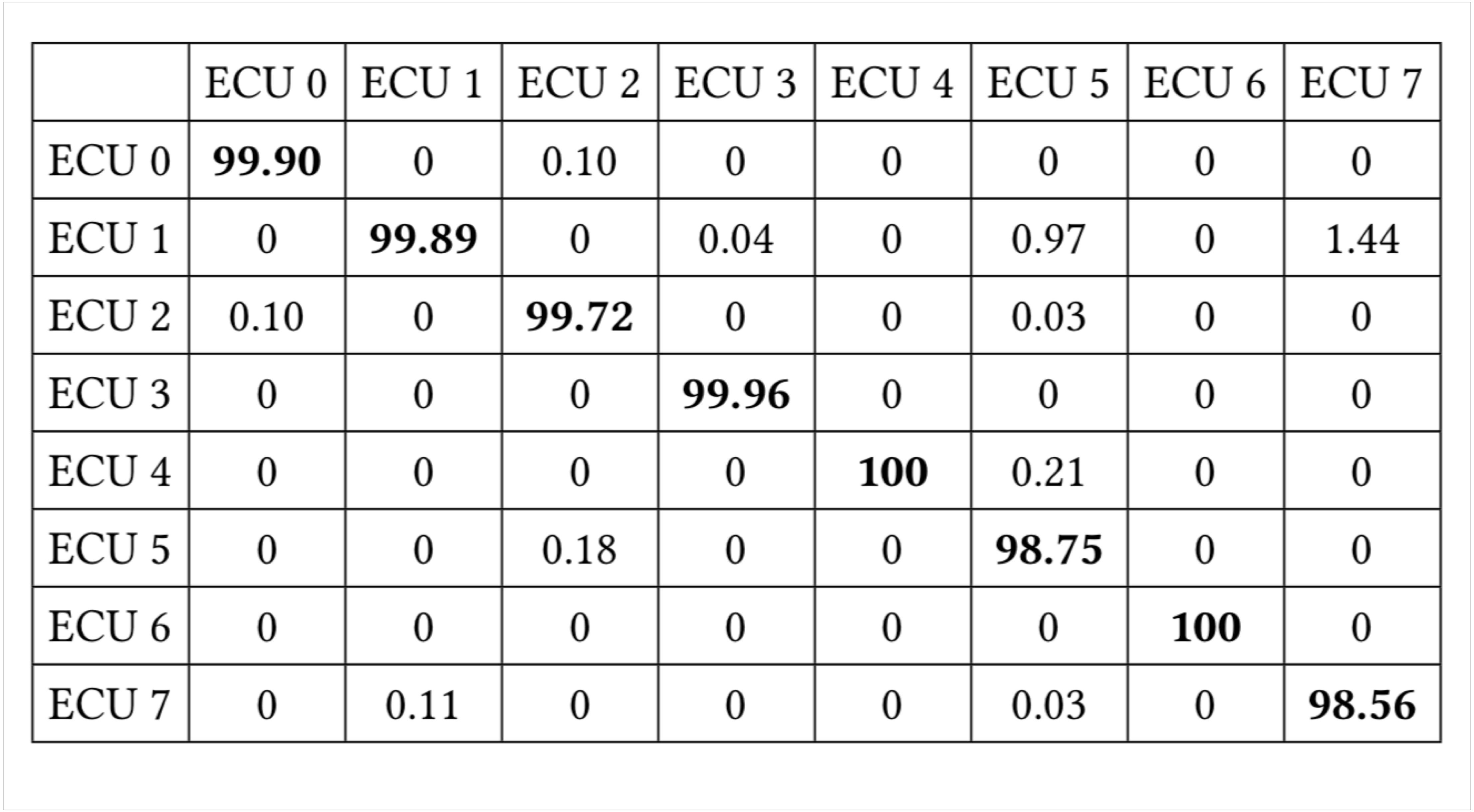
- Background Information
- How Scission Works
- **Implementation**
  - **Fingerprinting ECUs**
  - Detecting Compromised ECUs
- Conclusion

# Testbed of Arduinos



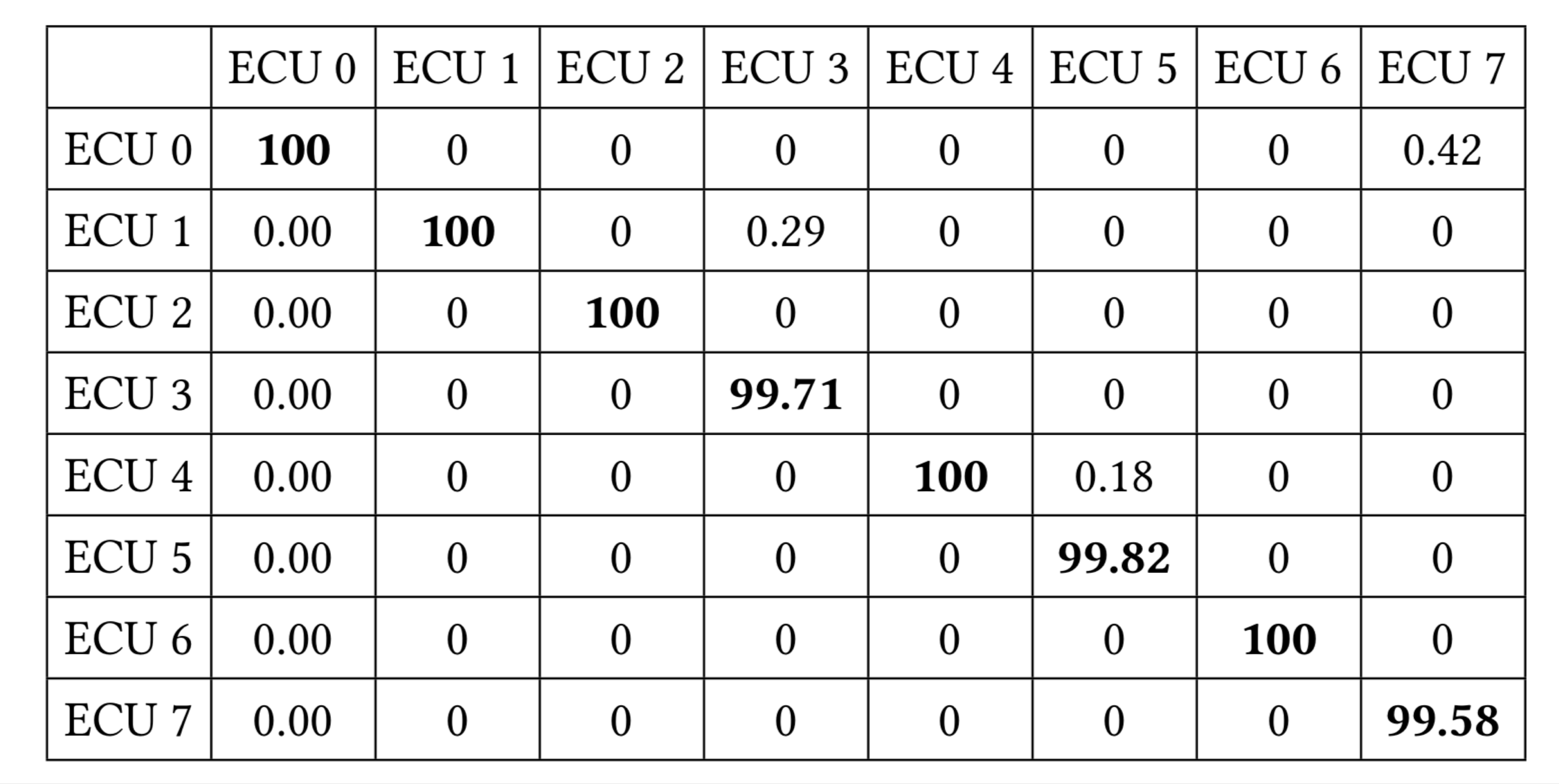
| | ECU 0 | ECU 1 | ECU 2 | ECU 3 | ECU 4 | ECU 5 | ECU 6 | ECU 7 | ECU 8 | ECU 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| ECU 0 | **100** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.42 |
| ECU 1 | 0 | **100** | 0 | 0.29 | 0 | 0 | 0 | 0 | 0 | 0 |
| ECU 2 | 0 | 0 | **100** | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ECU 3 | 0 | 0 | 0 | **99.71** | 0 | 0 | 0 | 0 | 0 | 0 |
| ECU 4 | 0 | 0 | 0 | 0 | **100** | 0.18 | 0 | 0 | 0 | 0 |
| ECU 5 | 0 | 0 | 0 | 0 | 0 | **99.82** | 0 | 0 | 0 | 0 |
| ECU 6 | 0 | 0 | 0 | 0 | 0 | 0 | **100** | 0 | 0 | 0 |
| ECU 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **100** | 0 | 0 |
| ECU 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **100** | 0 |
| ECU 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **99.58** |

# Fiat 500



| | ECU 0 | ECU 1 | ECU 2 | ECU 3 | ECU 4 | ECU 5 | ECU 6 | ECU 7 |
|---|---|---|---|---|---|---|---|---|
| ECU 0 | **99.90** | 0 | 0.10 | 0 | 0 | 0 | 0 | 0 |
| ECU 1 | 0 | **99.89** | 0 | 0.04 | 0 | 0.97 | 0 | 1.44 |
| ECU 2 | 0.10 | 0 | **99.72** | 0 | 0 | 0.03 | 0 | 0 |
| ECU 3 | 0 | 0 | 0 | **99.96** | 0 | 0 | 0 | 0 |
| ECU 4 | 0 | 0 | 0 | 0 | **100** | 0.21 | 0 | 0 |
| ECU 5 | 0 | 0 | 0.18 | 0 | 0 | **98.75** | 0 | 0 |
| ECU 6 | 0 | 0 | 0 | 0 | 0 | 0 | **100** | 0 |
| ECU 7 | 0 | 0.11 | 0 | 0 | 0 | 0.03 | 0 | **98.56** |

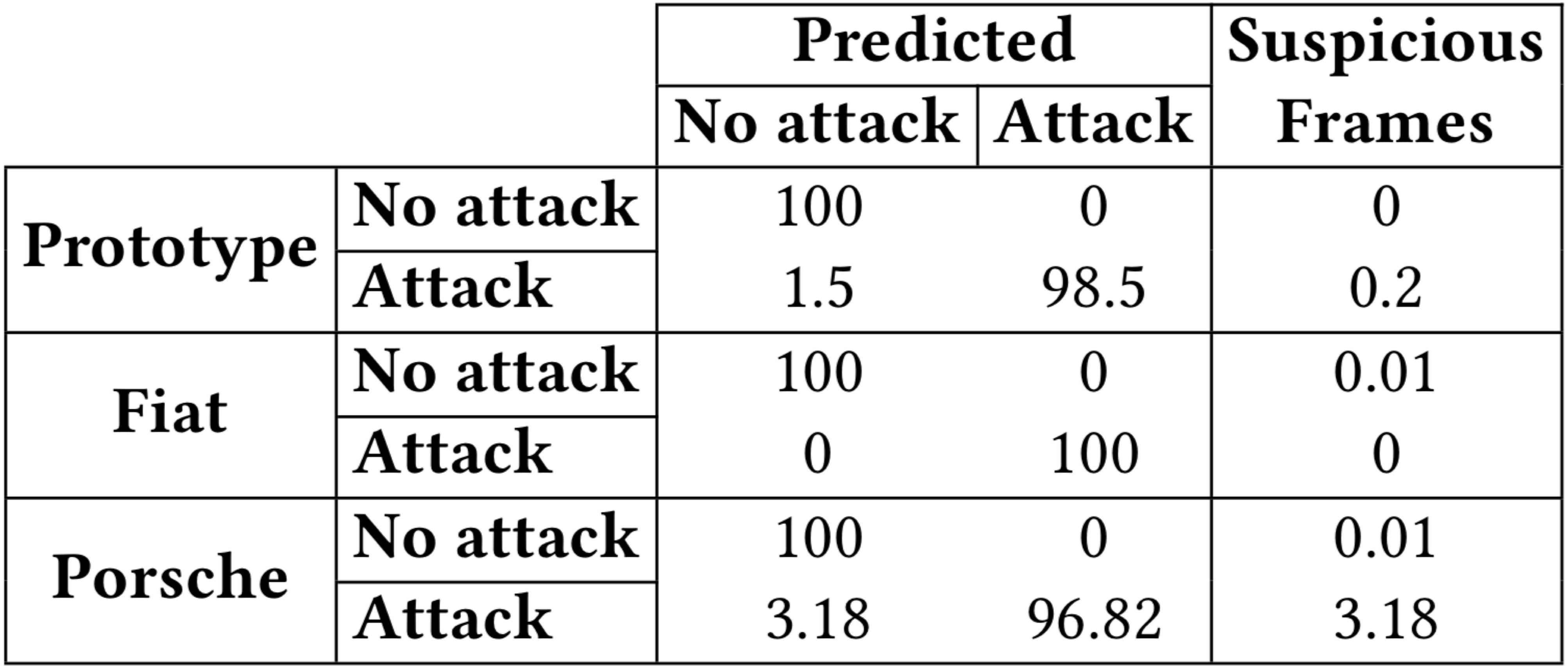
# Porsche Panamera



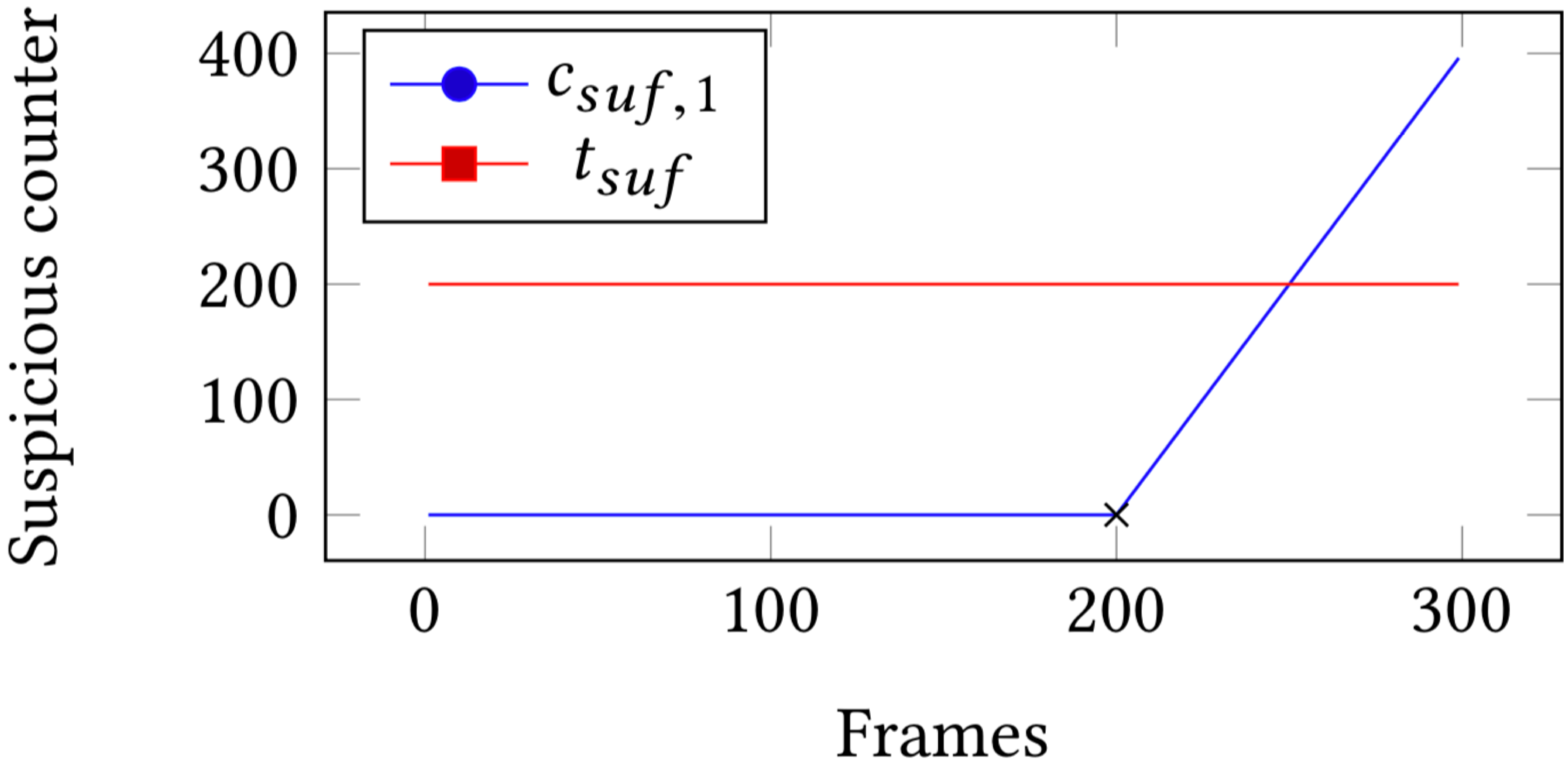
| | ECU 0 | ECU 1 | ECU 2 | ECU 3 | ECU 4 | ECU 5 | ECU 6 | ECU 7 |
|---|---|---|---|---|---|---|---|---|
| ECU 0 | **100** | 0 | 0 | 0 | 0 | 0 | 0 | 0.42 |
| ECU 1 | 0.00 | **100** | 0 | 0.29 | 0 | 0 | 0 | 0 |
| ECU 2 | 0.00 | 0 | **100** | 0 | 0 | 0 | 0 | 0 |
| ECU 3 | 0.00 | 0 | 0 | **99.71** | 0 | 0 | 0 | 0 |
| ECU 4 | 0.00 | 0 | 0 | 0 | **100** | 0.18 | 0 | 0 |
| ECU 5 | 0.00 | 0 | 0 | 0 | 0 | **99.82** | 0 | 0 |
| ECU 6 | 0.00 | 0 | 0 | 0 | 0 | 0 | **100** | 0 |
| ECU 7 | 0.00 | 0 | 0 | 0 | 0 | 0 | 0 | **99.58** |

# Outline

- Background Information
- How Scission Works
- **Implementation**
  - Fingerprinting ECUs
  - **Detecting Compromised ECUs**
- Conclusion



|  |  | Predicted |  | Suspicious Frames |
|---|---|---|---|---|
|  |  | No attack | Attack |  |
| Prototype | No attack | 100 | 0 | 0 |
|  | Attack | 1.5 | 98.5 | 0.2 |
| Fiat | No attack | 100 | 0 | 0.01 |
|  | Attack | 0 | 100 | 0 |
| Porsche | No attack | 100 | 0 | 0.01 |
|  | Attack | 3.18 | 96.82 | 3.18 |



Suspicious counter
400
300
200
100
0
0
100
200
300
Frames
$c_{suf,1}$
$t_{suf}$

# Outline

- Background Information
- How Scission Works
- Implementation
    - Fingerprinting ECUs
    - Detecting Compromised ECUs
- **Conclusion**

# Limitations

- If the attacker uses the identifier that Scission is familiar with, the attack will not be noticed.
- If the characteristics of the CANBUS is changed, Scission cannot then identify the attacks.
- The attacker can also send messages infrequently to not exceed the suspicious frames threshold.

# Conclusion

- Scission is an IDS for inter-car communication.
- Utilizes the signal characteristics found in the electronic data of a CAN Network.
- Can account for unmonitored ECUs and additional ECUs