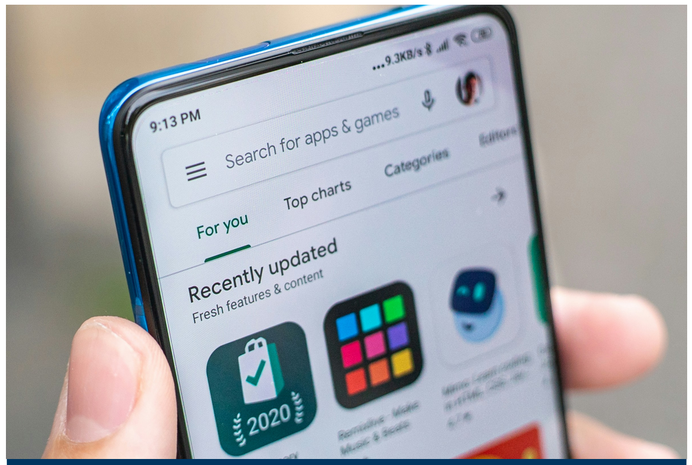

# Vulnerability, Where Art Thou?

## An Investigation of Vulnerability Management in Android Smartphone Chipsets

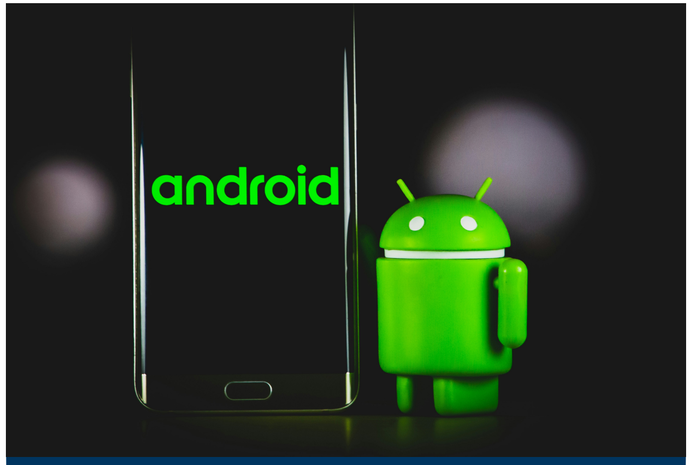
**Daniel Klischies**, Philipp Mackensen, Veelasha Moonsamy

SECURITY AND PRIVACY
OF UBIQUITOUS SYSTEMS

# Smartphone security: Multi-layered complexity

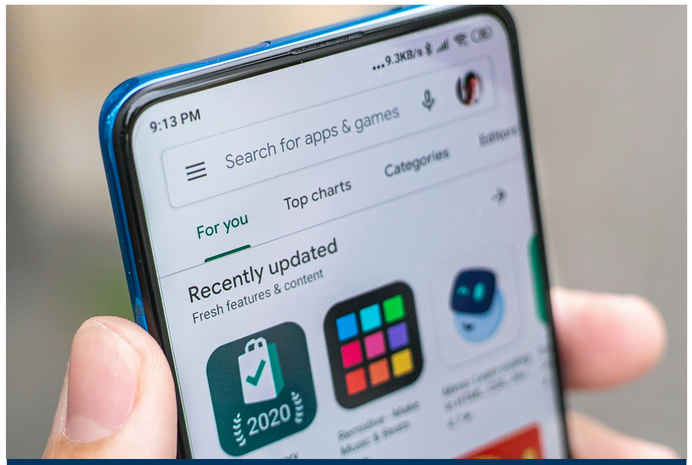



Apps

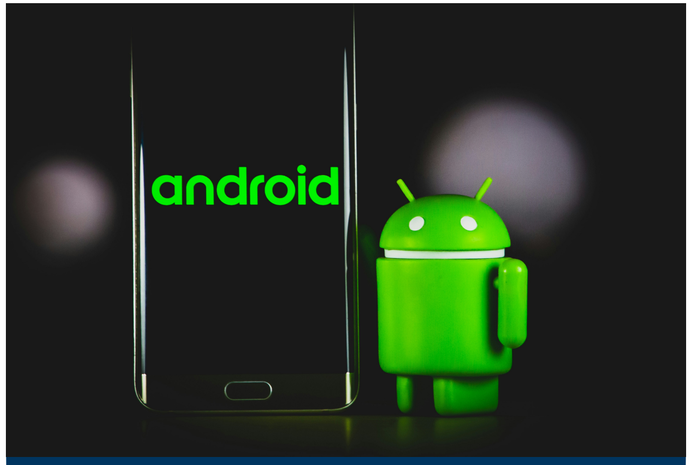



Android

# Smartphone security: Multi-layered complexity




Apps




Android

Chipset

# Smartphone security: Multi-layered complexity

**Open questions:**

- Do different chipsets share vulnerabilities?
- Who discovers chipset vulnerabilities?
- What are typical timeframes until vulnerabilities are mitigated?

**And many more**


Chipset

# Smartphone chipsets

## Components

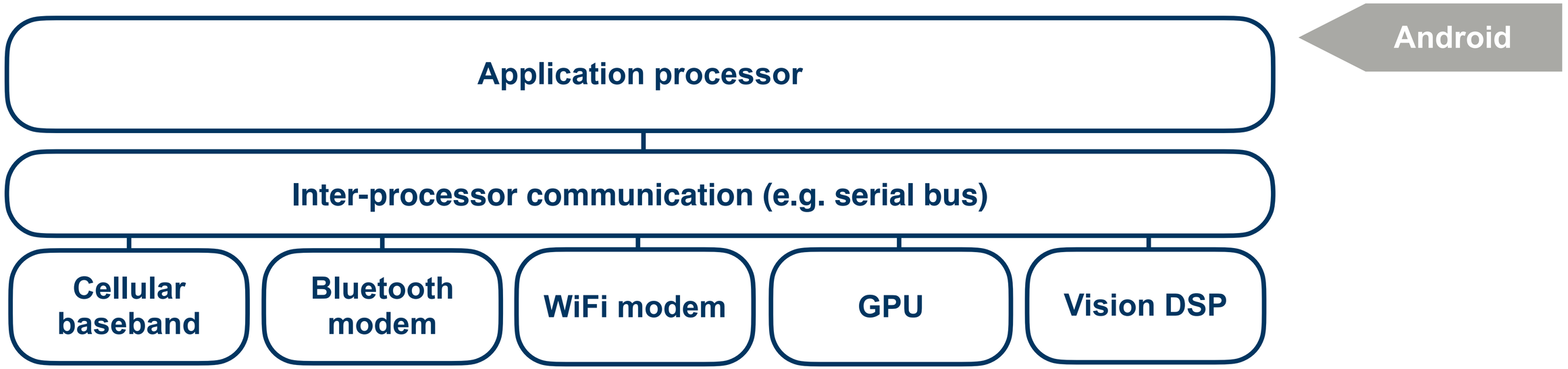

Supplied by:

Chipset manufacturers

Smartphone manufacturers

# Smartphone chipsets

## Components

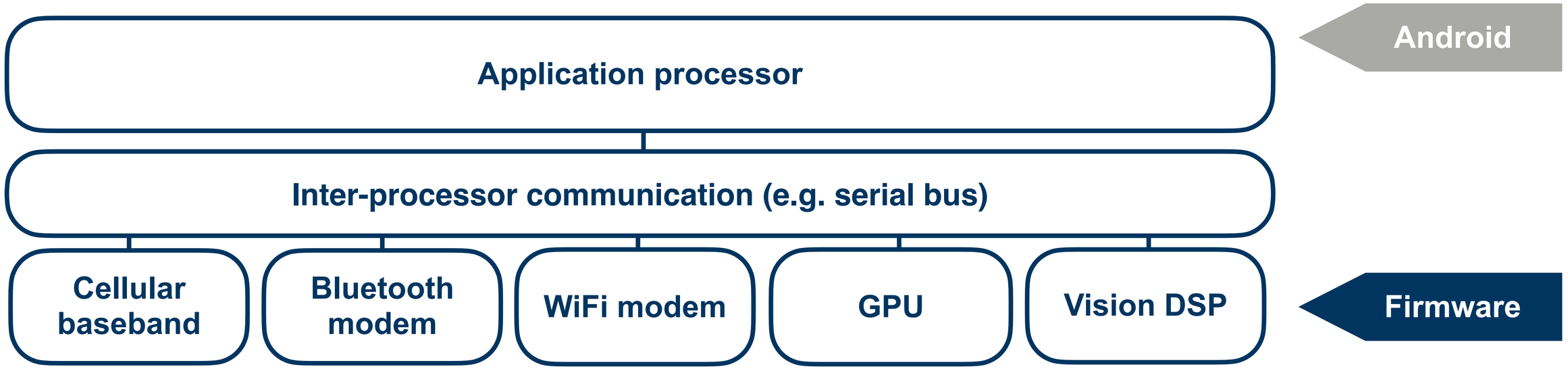



Supplied by:

Chipset manufacturers | Smartphone manufacturers

# Smartphone chipsets

## Components

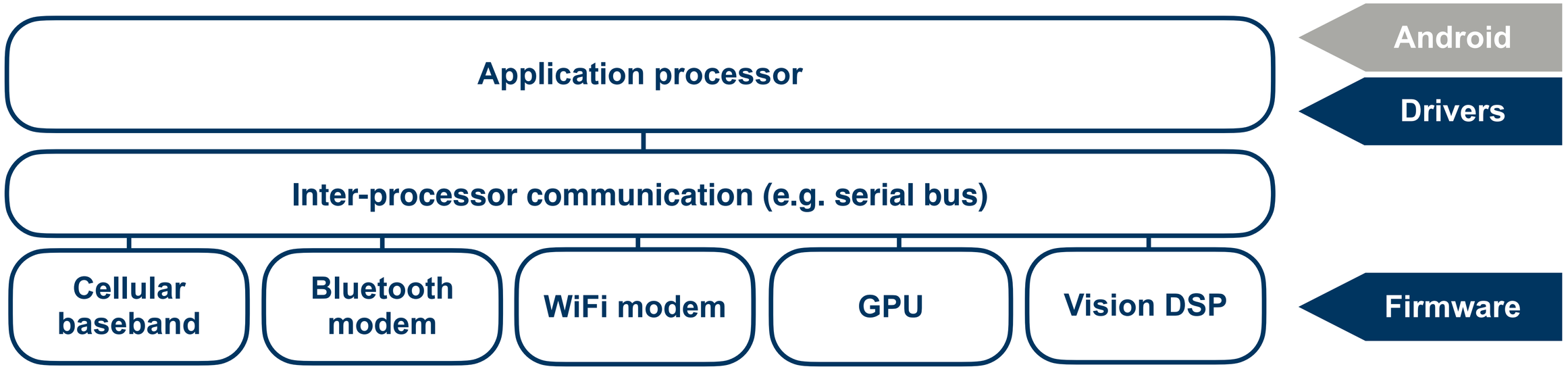



Supplied by:

Chipset manufacturers | Smartphone manufacturers

# Smartphone chipsets

## Components

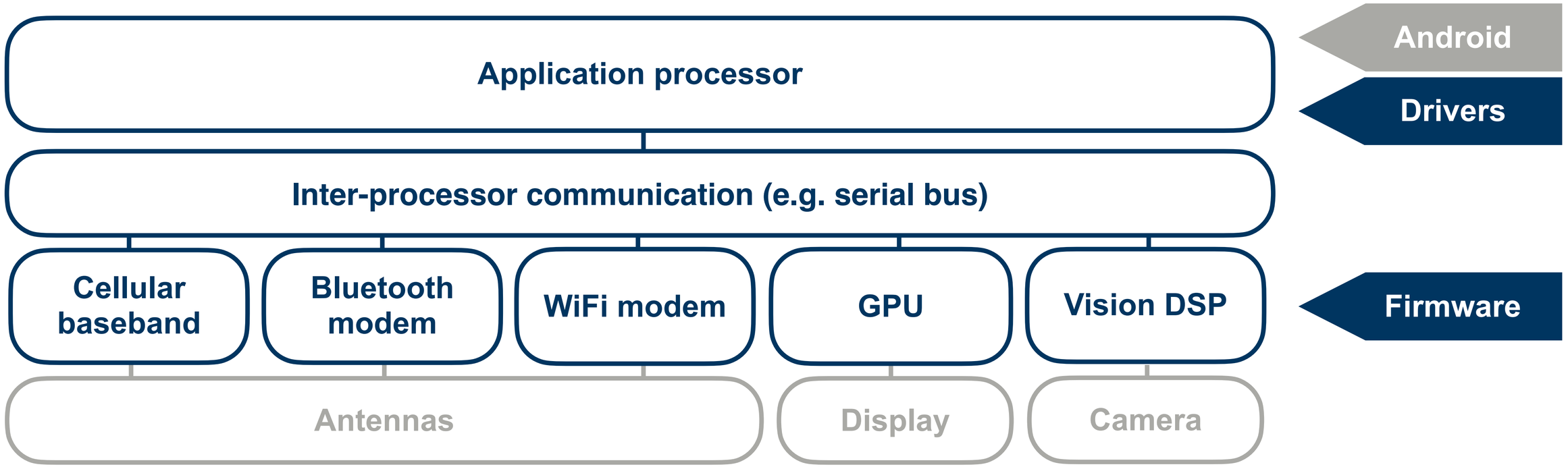



Supplied by:

Chipset manufacturers | Smartphone manufacturers

# Smartphone chipsets

## Components

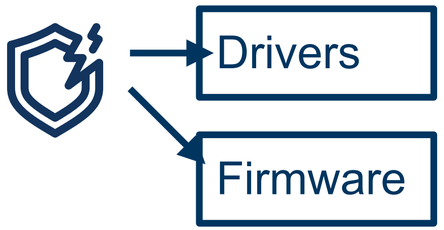



Supplied by:

Chipset manufacturers | Smartphone manufacturers

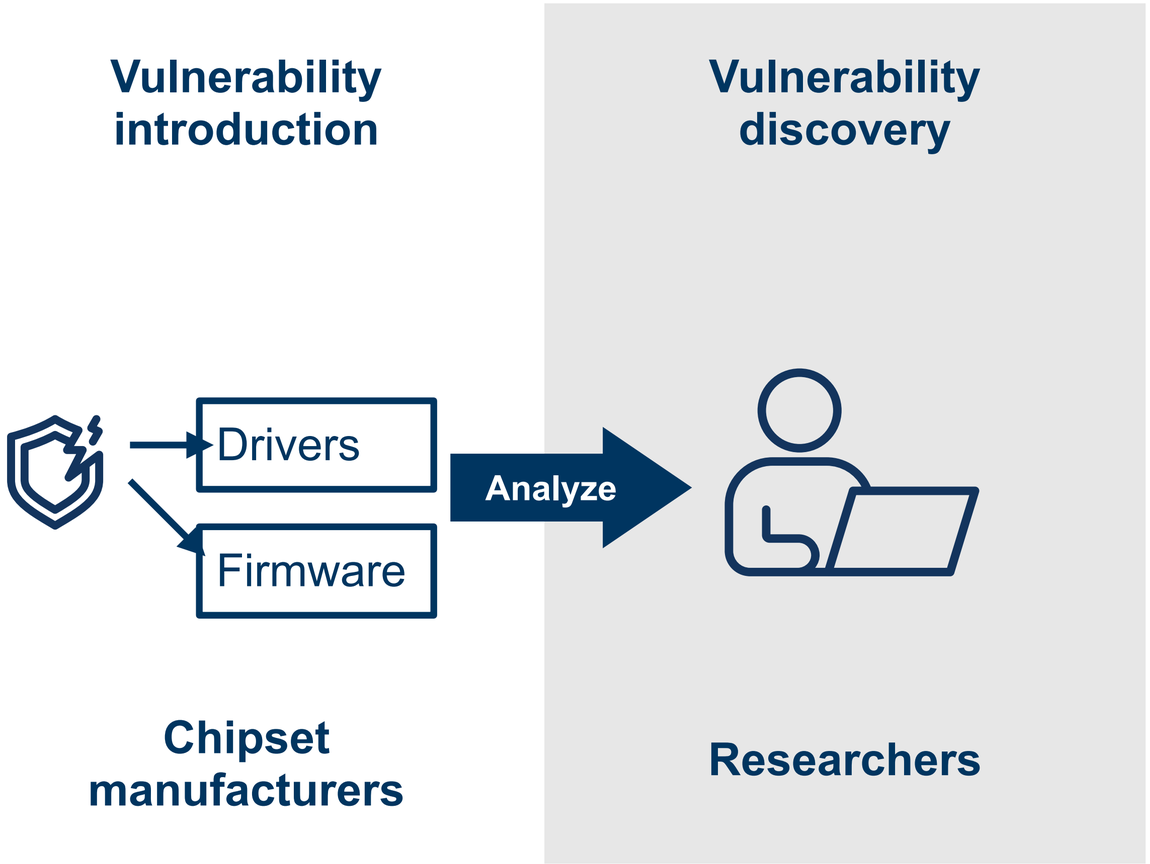
# Chipset vulnerability lifecycle

**Vulnerability introduction**

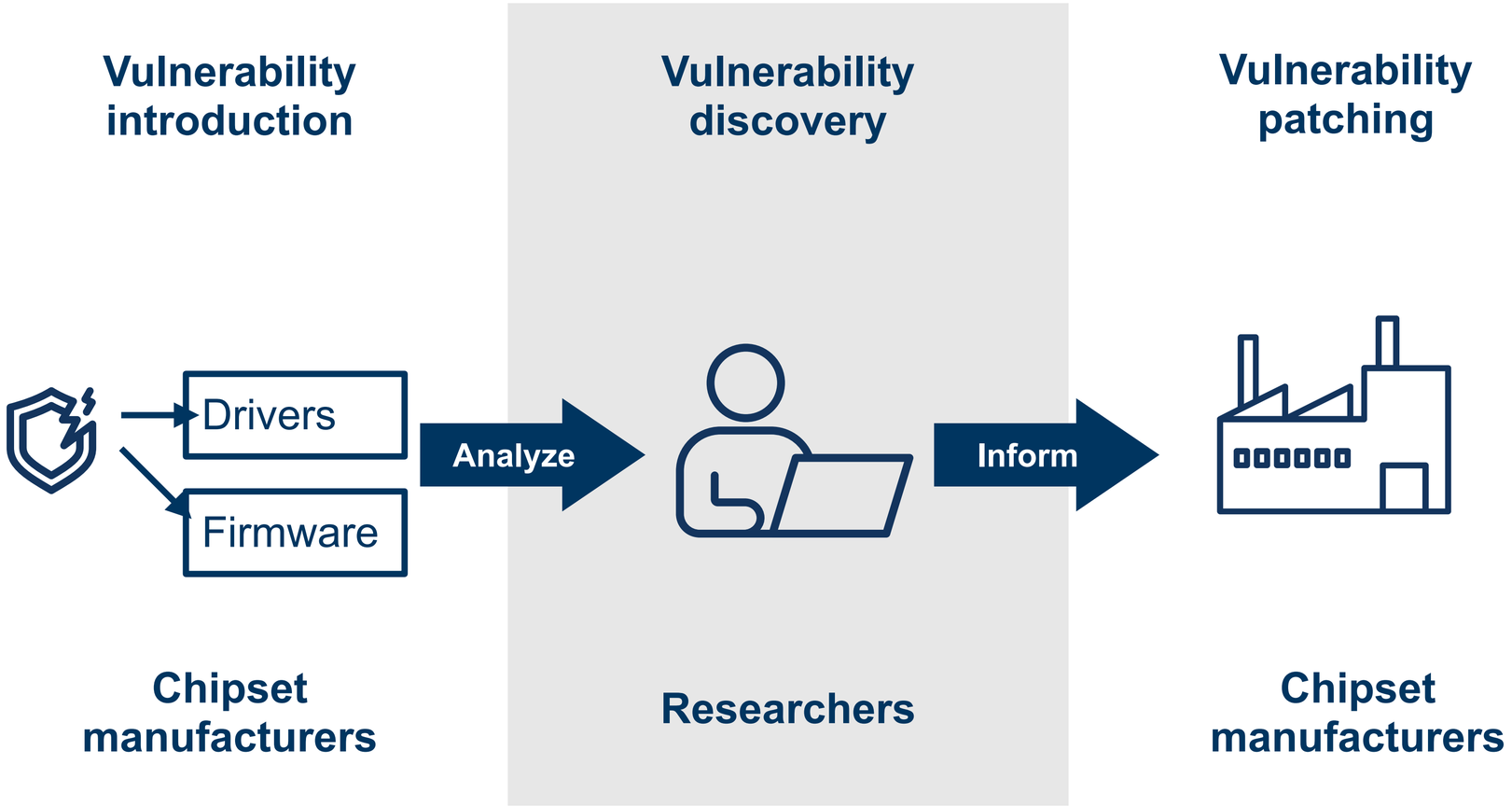



**Chipset manufacturers**

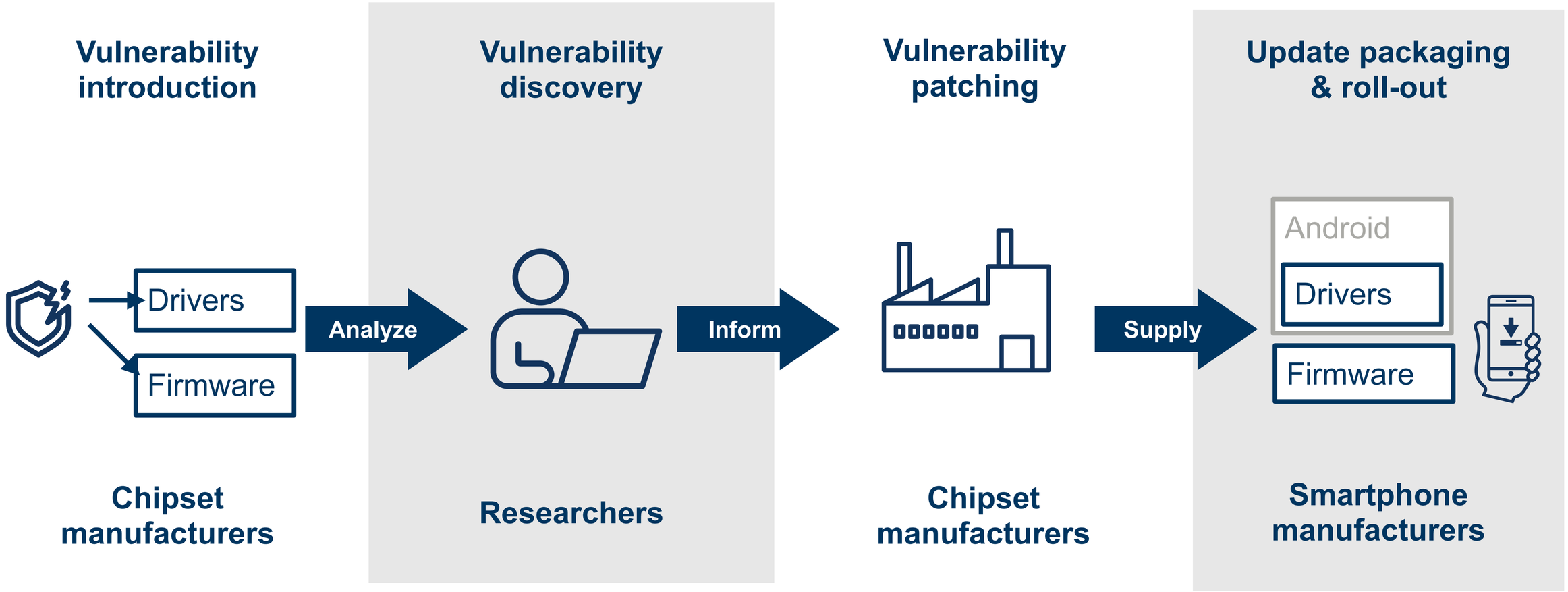
# Chipset vulnerability lifecycle



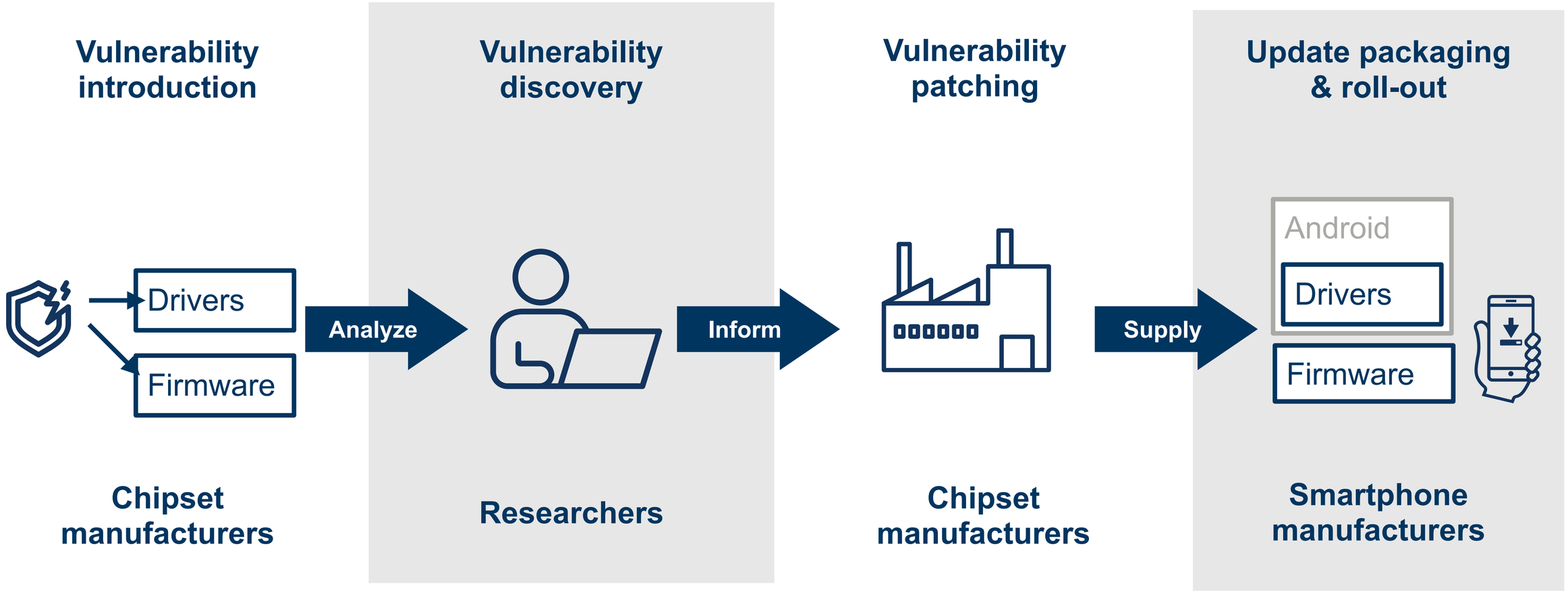
# Chipset vulnerability lifecycle



# Chipset vulnerability lifecycle



# Chipset vulnerability lifecycle




**→ Challenge: Information is scattered across websites of involved companies**

# Our knowledge base

- Android security bulletins
- Chipset manufacturer websites
- National Vulnerability Database
- Smartphone update changelogs
- Product databases

**3,600+**
Vulnerabilities

**18,000+**
Updates

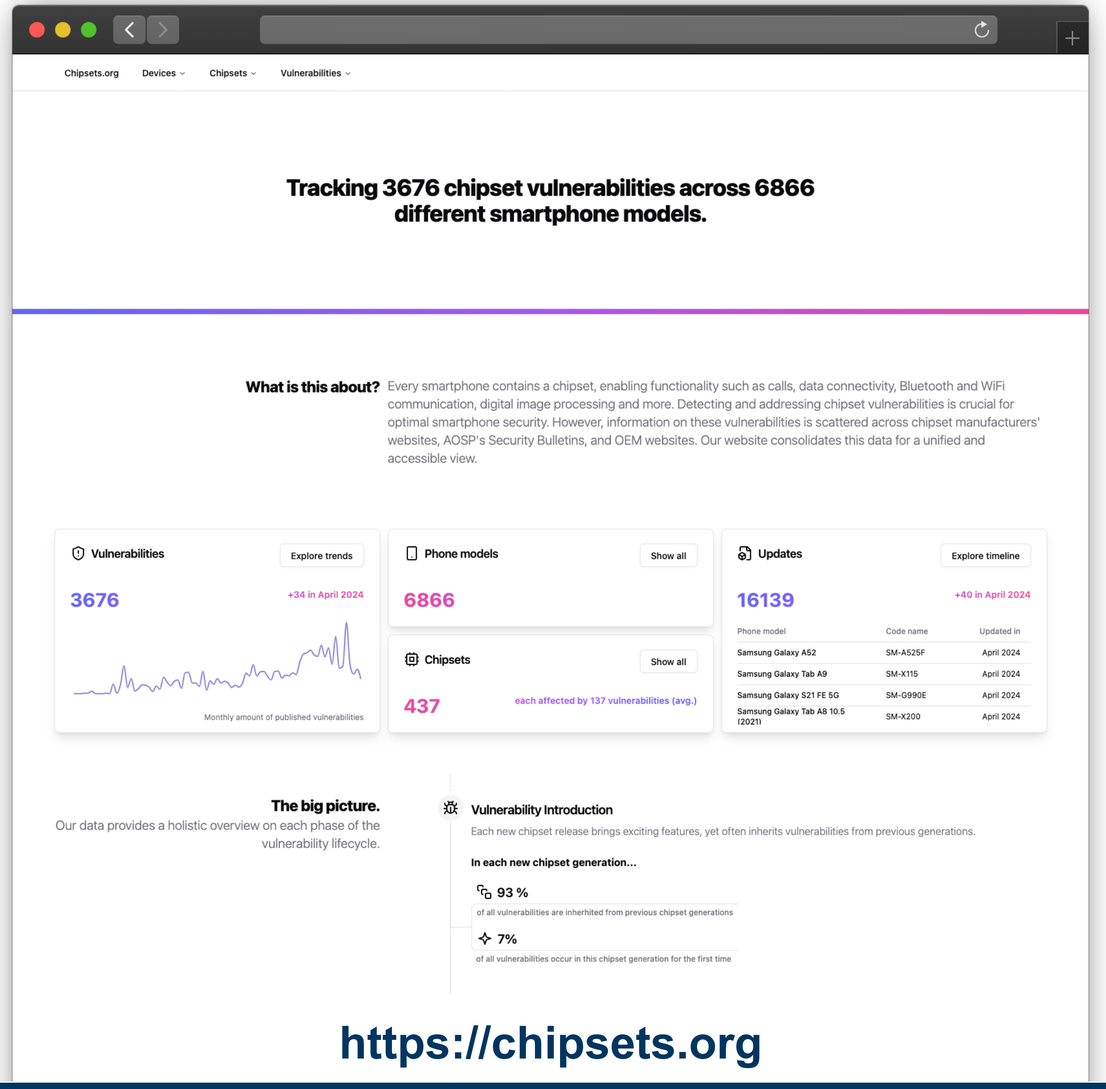
**430+**
Chipset models

Qualcomm, Samsung, MediaTek, Unisoc

**6,800+**
Phone models

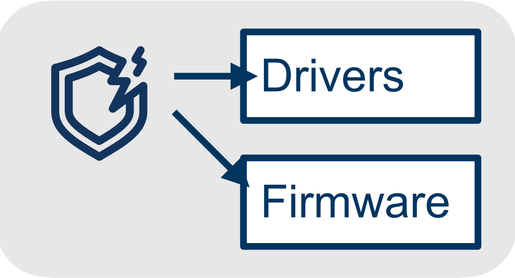
# Our knowledge base

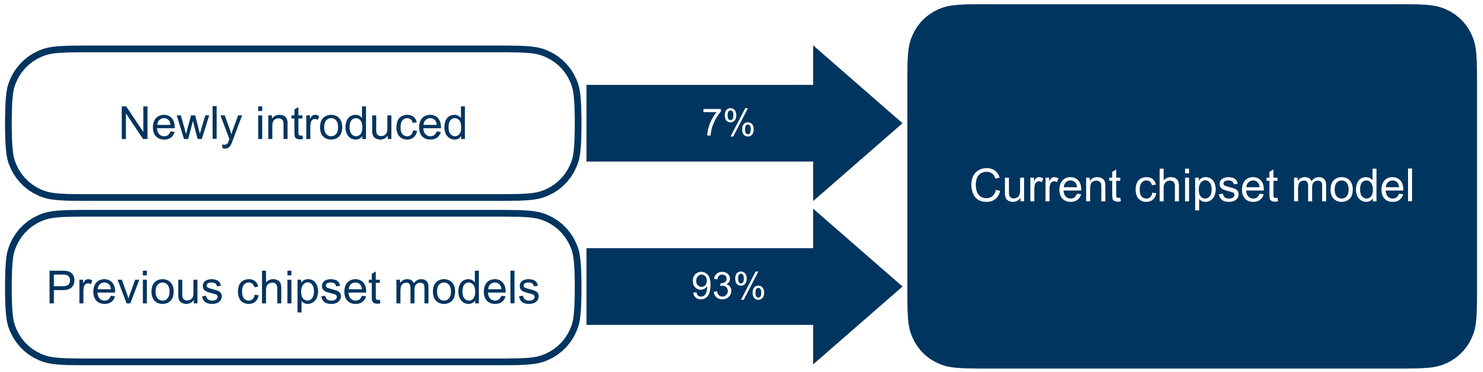
- Android security bulletins
- Chipset manufacturer websites
- National Vulnerability Database
- Smartphone update changelogs
- Product databases



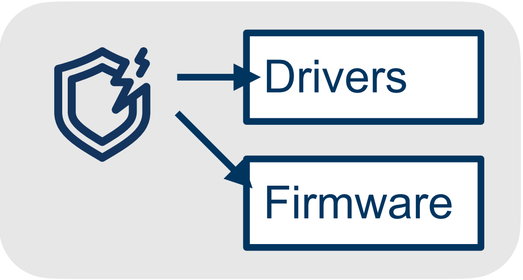

**https://chipsets.org**

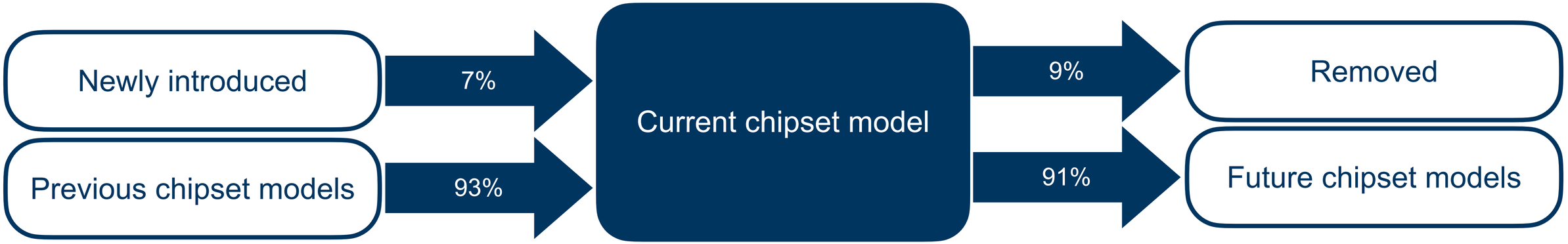
# Vulnerability introduction



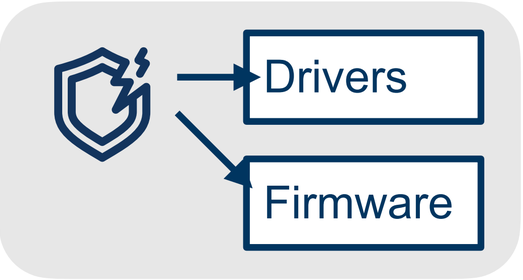



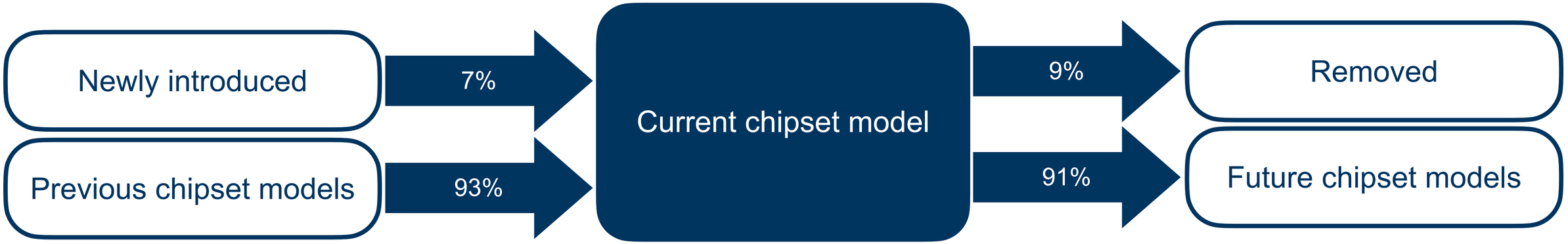
# Vulnerability introduction



# Vulnerability introduction



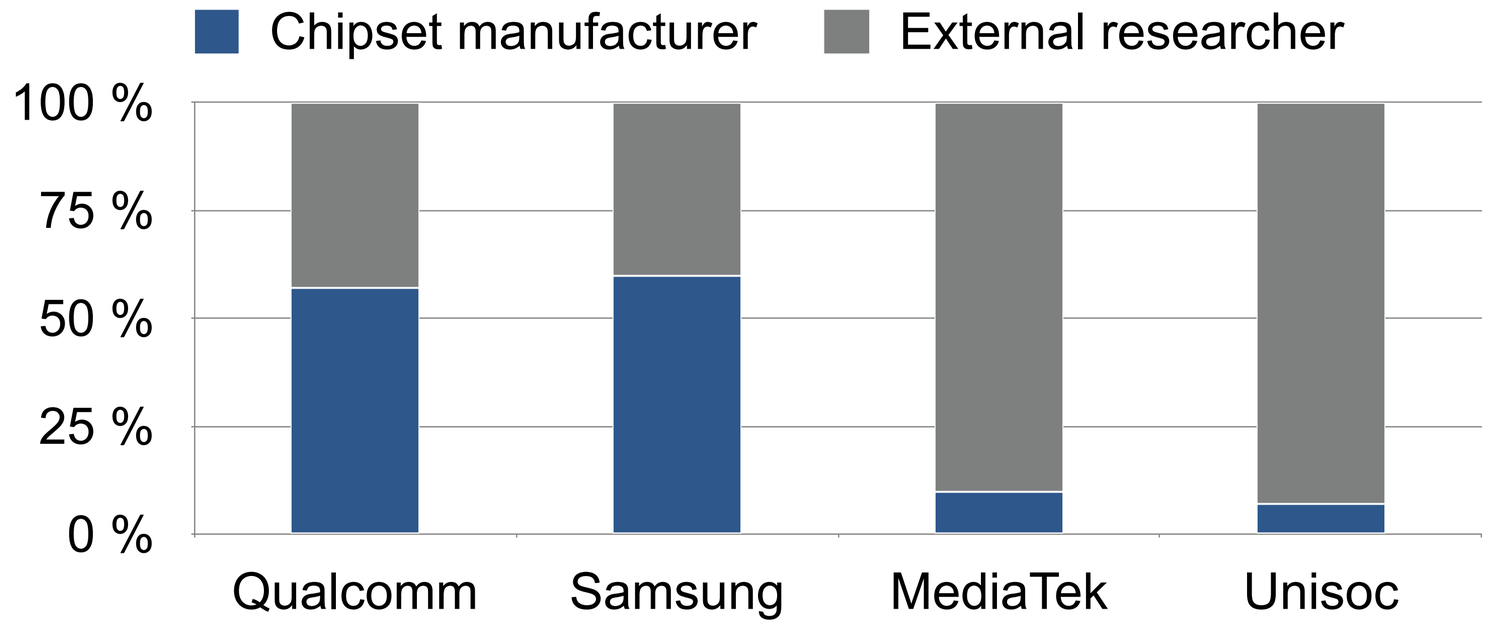




**Takeaways:**

- Analyzing **legacy features** still yields **new vulnerabilities**
- A lot of code is **shared** between chipset models
  - Requires time consuming assessment which models include vulnerable code

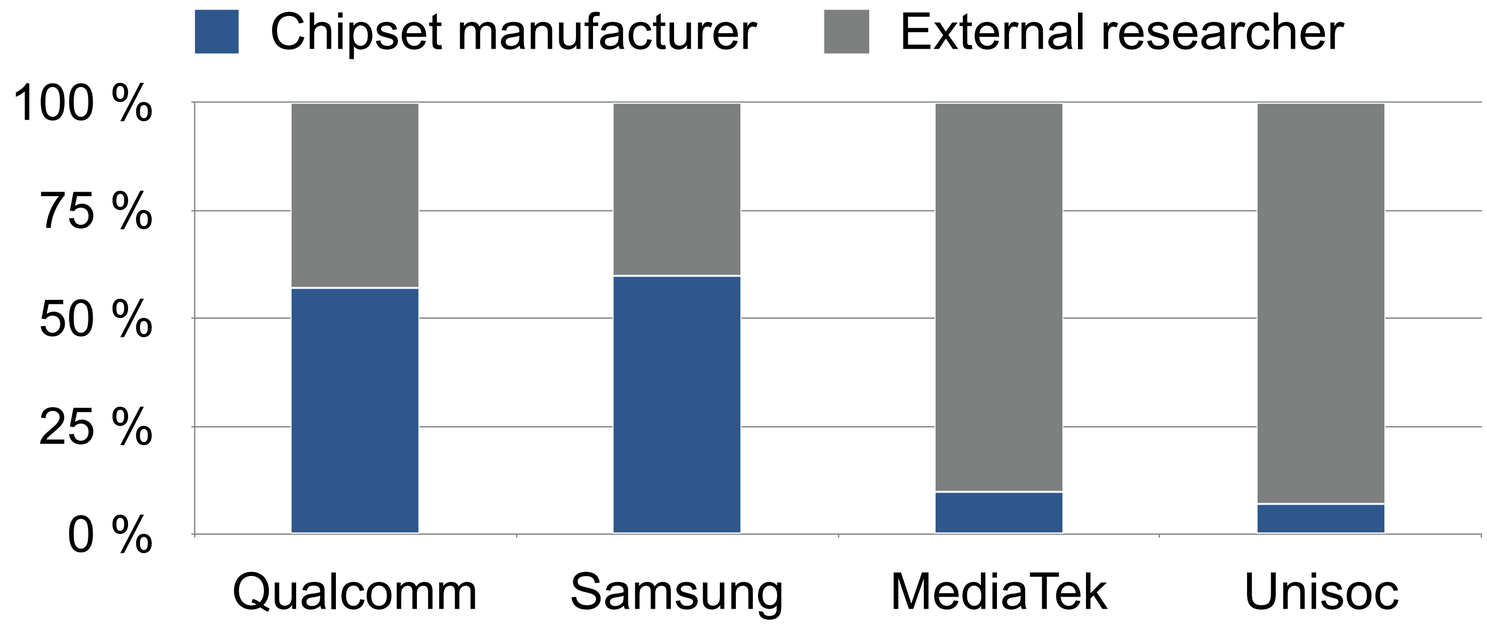
# Vulnerability discovery

## Who discovers most vulnerabilities post release (2023)?



# Vulnerability discovery

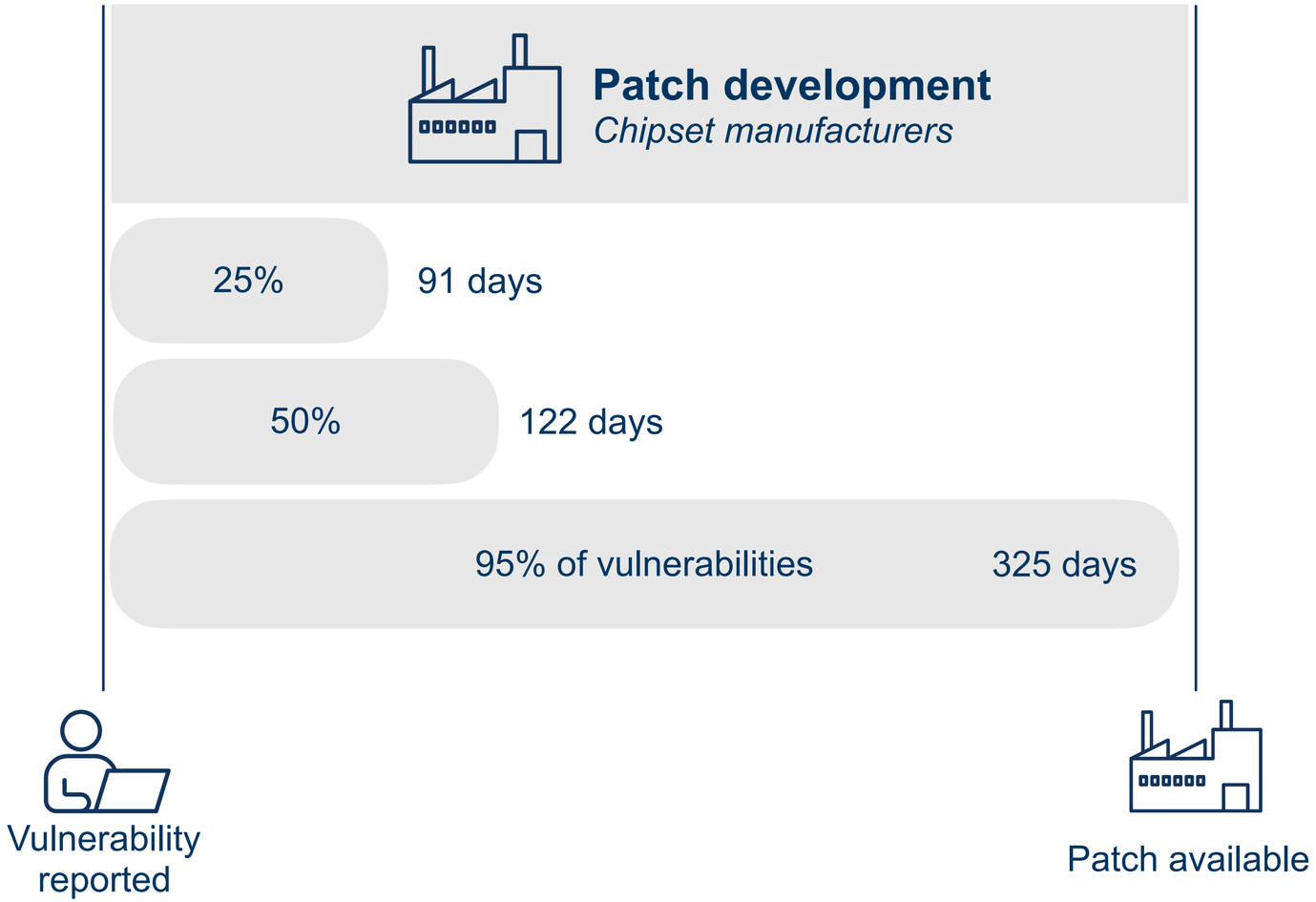
## Who discovers most vulnerabilities post release (2023)?



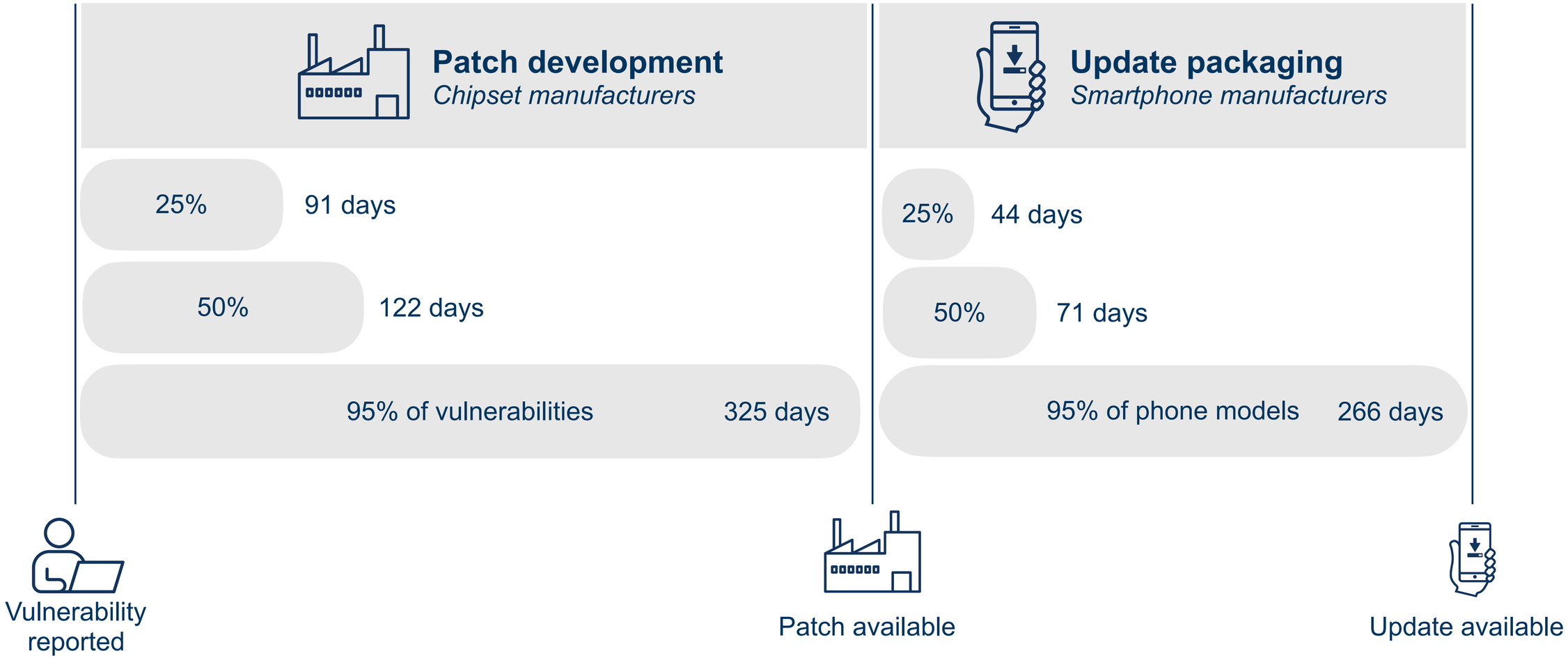

**Takeaways:**

- Generally high reliance on external researchers
- Disclosure processes for external researchers exist & reports are taken seriously

# Patch & Update timeline



# Patch & Update timeline

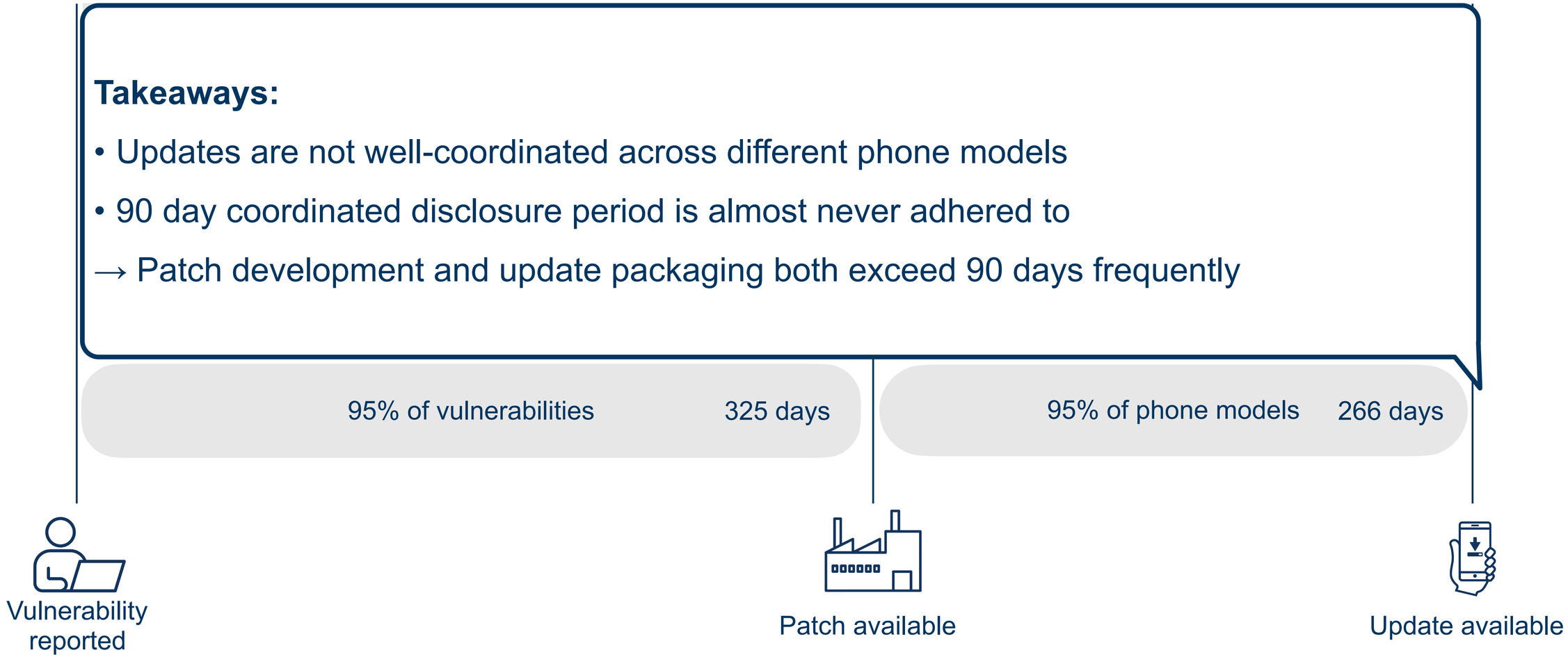


# Patch & Update timeline

**Takeaways:**

- Updates are not well-coordinated across different phone models
- 90 day coordinated disclosure period is almost never adhered to

→ Patch development and update packaging both exceed 90 days frequently



# Additional use cases

**Identify trends and avenues for future research**
→ Which components yield the most severe vulnerabilities?
→ Where do we see few vulnerabilities?

# Additional use cases

**Identify trends and avenues for future research**
→ Which components yield the most severe vulnerabilities?
→ Where do we see few vulnerabilities?

**Make an informed selection of evaluation devices**
→ Many chipsets have almost the same set of vulnerabilities
→ We offer a tool to estimate and select diverse sets of phone models

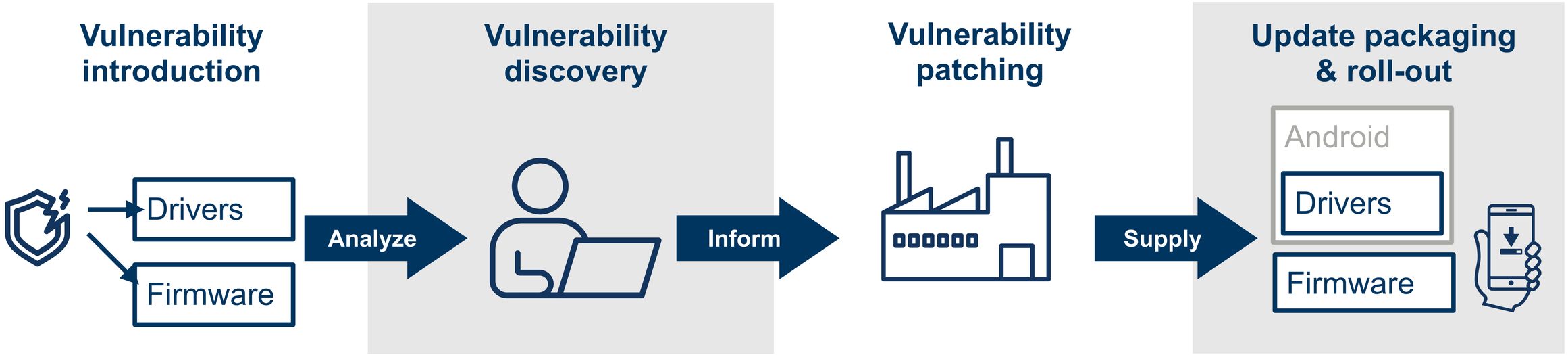
# Additional use cases

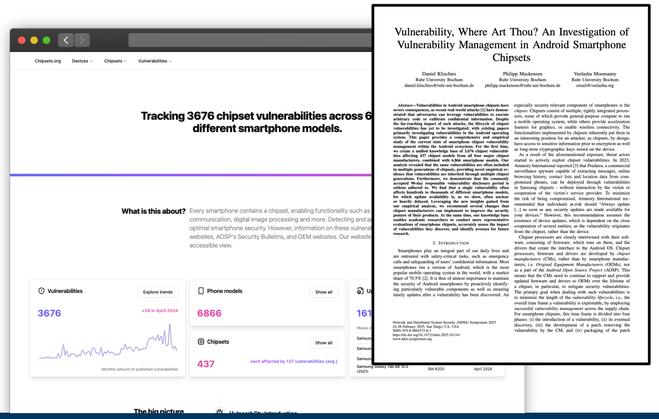
**Identify trends and avenues for future research**
→ Which components yield the most severe vulnerabilities?
→ Where do we see few vulnerabilities?

**Make an informed selection of evaluation devices**
→ Many chipsets have almost the same set of vulnerabilities
→ We offer a tool to estimate and select diverse sets of phone models

**Determine how widespread a recently found vulnerability is**
→ List all chipsets and smartphones affected by a vulnerability

# Summary





Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone Chipsets

**In the paper & on https://chipsets.org:**

What are the most affected components?

Differences between firmware and drivers

Comparison to other ecosystems

…