

# ACM WiSec 2024

## Trip report

Seoul, Korea  
May 27 - May 30, 2024



## 개요

2024년 5월 서울에서 개최된 WiSec에 참여하였다. 본 컨퍼런스에서는 대부분의 논문들이 통신과 관련된 보안을 해결하기 위한 기술을 제안하는 주제였다. 통신 쪽의 개념은 대부분 모르지만, 어떤 기술들이 있는지, 통신 쪽에는 어떤 보안 문제가 있는지 볼 수 있는 좋은 기회였다. 본 레포트에서는 WiSec에서 발표된 내용 중 어떤 기술을 제안하고 있는지, 그 목적은 무엇인지, 그 기술을 통해 어떤 것을 보호할 수 있는지 위주로 정리하였다.

# Paper

## 1. Covert Communications with Simultaneous Multi-Modal

이 논문은 통신 링크의 covertness를 강화하기 위한 기법을 제안한 것으로, 네트워크 위협에서 covertness하고 감지가 덜 되도록 하여 공격자로부터 통신의 존재 자체를 숨기는 방법을 제안한다. covertness를 높이는 것을 우선으로 하여 두 노드 사이의 통신을 숨기는 joint detection threshold optimization 기술을 사용한다. 한 노드가 여러 모드를 동시에 사용함으로써 데이터 처리량을 줄이지 않고 더 높은 데이터 처리량을 달성할 수 있다는 것을 이용하여 각 모드에 사용되는 전송 전력을 제어하면서 다른 노드에서 필요한 최소 데이터 처리량을 보장하는 모델을 개발하였다. 이를 통해 합법적인 통신 링크의 covertness를 PDEP 측면에서 정량화하였다. PDEP를 극대화하여 전송 전력 값을 최적화하는 기술을 도입하였다. 이 기술을 통해 기존 방법보다 covertness를 56% 향상시킴을 증명하였다.

여기서는 통신이 이루어 지는 것 자체, 즉 covertness를 숨김으로써 공격자가 감지하지 못하도록 하는 joint detection threshold optimization을 제안하였다. 여기서는 단일 통신 링크에 대해 여러 전송 모드를 동시에 사용하여 전송의 효율을 떨어뜨리지 않으면서 covertness를 높이고 있다. 이를 통해 잠재적 적대자로부터 통신의 존재 자체를 기존보다 56% 향상시켰다고 한다.

### 3 SYSTEM MODEL

- Alice communicates with Bob in multiple transmission slots.
- $x^{(k)}[n] \sim \mathcal{C}(0,1)$  is the transmitted data symbol for the  $n^{\text{th}}$  channel use.
- Signal received at Bob/Willie(W) for modality  $k$  -  $y_t^{(k)}[n] = \sqrt{p^{(k)}}h_t^{(k)}x^{(k)}[n] + n_t^{(k)}[n]$  where  $t \in \{B, W\}$  and  $n \in \{0, 1, 2, \dots, L\}$
- Rate at Bob for modality  $k$  -  $R^{(k)} = \Omega^{(k)} \log_2(1 + \text{SNR}_B^{(k)}) = \Omega^{(k)} \log_2\left(1 + \frac{p^{(k)} |h_B^{(k)}|^2}{\Omega^{(k)} N_{0,B}}\right)$

Figure 1 – Network model for covert communication with simultaneous multi-modal transmission.

### 5 OPTIMIZATION PROBLEM AT ALICE

- Alice's goal–maximize covertness (i.e. DEP)
- Constraints– 1) minimum data rate required at Bob, 2) per modality maximum power budget
- Action Space–Transmit power for each modality  $P^{(k)}$

$$\begin{aligned} \max_{P^{(k)}} \quad & P_{\text{DEP}} \\ \text{s.t.} \quad & P^{(k)} \leq P_{\text{max}}^{(k)}, k \in \{1, 2\}, \\ & R_B \geq R_{B, \text{reqd}} \end{aligned}$$

### 4 DETECTION MODEL AT WILLIE

- Hypothesis test for each modality as-  $\mathcal{H}_0^{(k)}: y_W^{(k)}[n] = n_W^{(k)}[n], n = 1, \dots, L$   
 $\mathcal{H}_1^{(k)}: y_W^{(k)}[n] = \sqrt{p^{(k)}}h_W^{(k)}x^{(k)}[n] + n_W^{(k)}[n], n = 1, \dots, L$
- Average received signal strength at Willie -  $\bar{y}_W^{(k)} = \frac{1}{L} \sum_{n=1}^L |y_W^{(k)}[n]|^2$
- Threshold test -  $\bar{y}_W^{(k)} \underset{\mathcal{D}_0^{(k)}}{\overset{\mathcal{D}_1^{(k)}}{\geq}} \delta^{(k)}$  Overall decision is made as-  $\mathcal{D}_0 = \{\mathcal{D}_0^{(1)} \text{ and } \mathcal{D}_0^{(2)}\}$   $\mathcal{D}_1 = \{\mathcal{D}_1^{(1)} \text{ or } \mathcal{D}_1^{(2)}\}$
- Covertness is quantified via Detection Error Probability which is defined as-  $P_{\text{DEP}} \triangleq \frac{1}{2}P_{\text{MD}} + \frac{1}{2}P_{\text{FA}} = \frac{1}{2} \left( P_{\text{MD}}^{(1)} P_{\text{MD}}^{(2)} \right) + \frac{1}{2} \left( P_{\text{FA}}^{(1)} + P_{\text{FA}}^{(2)} - P_{\text{FA}}^{(1)} P_{\text{FA}}^{(2)} \right)$

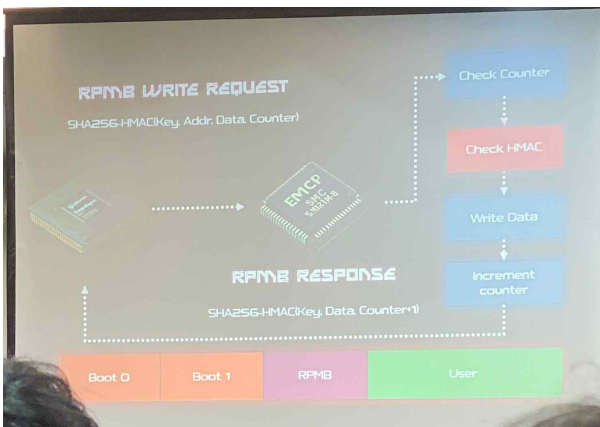
### 12 CONCLUSION

- We have shown a computationally efficient way to evade detection while using two wireless communication technologies simultaneously.
- The proposed technique can be applied to any combination of two modalities.
- Future work–
  - optimizing transmit bandwidth,
  - more than two simultaneous modalities,
  - network of friendly transmitters and receivers evading multiple adversaries.

## 2. Keyless Entry: Breaking and Entering eMMC RPMB with EMFI


이 논문은 storage의 RPMB에 저장된 데이터를 전자기 펄스 주입(EMFI)을 통해 하드웨어의 의도치 않은 동작을 발생시켜 RPMB에 임의의 데이터를 작성해 RPMB의 인증체계를 깨뜨릴 수 있다는 것을 보여준 논문이다.

Storage의 Replay Protected Memory Block (RPMB)은 인증을 통해 데이터 무결성이 보장되는 안전한 영역을 제공한다. RPMB에 데이터를 쓰려면 암호화 해시 함수, 즉 SHA256을 사용한 키-해시 메시지 인증 코드(HMAC)를 사용하여 인증해야 한다. RPMB 인증이 공유 전 사전 키의 기밀성에만 의존한다. RPMB 읽기 요청 명령을 발행하면 누구나 RPMB 데이터의 내용을 읽을 수 있어, 일반 사용자에게 변경할 수 없는 정보를 저장하는 데 일반적으로 사용된다. 본 논문에서는 이 인증 체계를 깨뜨려 공격자가 사전 공유된 키를 알지 못하고도 RPMB의 데이터를 덮어쓸 수 있게한다. storage에 EMFI를 적용하였다. 외부 소스에서 전원을 공급받기 때문에, 하드웨어 변형없이 컨트롤러의 코어 전압(Vddi)과 메모리 주변 장치(Vcc)를 쉽게 조작하여 전압 글리칭을 적용하여 RPMB에 데이터를 덮어쓸 수 있었다.




# TARGETS


- Three different eMMC devices
- Responsible disclosure
  - Details will be released in September 2024



## TARGET #1



## TARGET #2



## TARGET #3

TARGET #1		TARGET #2		TARGET #3	
eMMC	441	eMMC	51	eMMC	50
Part no.	Cortex M3	Part no.	Cortex M7	Part no.	Cortex M3
Architecture	ARMv7-M	Architecture	ARMv7-M	Architecture	ARMv7-M
MPU	Disabled	MPU	Disabled	MPU	Disabled
VTOR	0x40000	VTOR	0x60000000	VTOR	0x40000

## 3. Uncovering Security Vulnerabilities in Real-world Implementation and Deployment of 5G Messaging Services

5G 메시징 서비스에 대한 보안 연구로 5G 메시징 활성화 장치에서 Man-In-The-Middle (MITM) 공격, 제로 클릭 원격 정보 유출, 휴대폰 저장 공간 고갈 및 모바일 데이터 소비, 그리고 서비스 거부(DoS) 공격이 일어날 수 있음을 보였다.

5G 메시징 서비스는 Global System for Mobile Communications Association (GSMA)의 Rich Communication Service (RCS)와 3rd Generation Partnership Project (3GPP)의 IP Multimedia Subsystem (IMS)를 기반으로 이루어진다. 본 논문에서는 IMS를 기반으로 하는 5G 메시징에서 잠재적인 보안 위험은 무엇이 있는지 실제 5G 메시징 서비스에서 잠재적 취약점을 체계적으로 감지하고 확인할 수 있는 반자동 도구인 Sipano를 설계하여 확인하였다. 이 논문은 전날 banquet에서 만난 분들이 발표한 논문이어서 들었는데, 이 발표에서 질문으로는 해당 기술이 중국에서만 사용되는 기술이어서 다른 곳에도 적용할 수 있는지에 대한 질문이 있었다.

