

A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons

논문 저자

Tamara Denning, Cynthia Matuszek, Karl Koscher,
Joshua R. Smith, Tadayoshi Kohno

UbiComp 2009

발표자 안명균 · 학번 80241152
기계공학과 DRCL · 2026.09.16

목차

01	Motivation	p.3–9
02	Problem	p.10–13
03	Related Work	p.14–17
04	Method & Evaluation	p.18–32
05	Contribution	p.33–35
06	Future Work	현재적 비교·후속 연구 제안 p.36–42

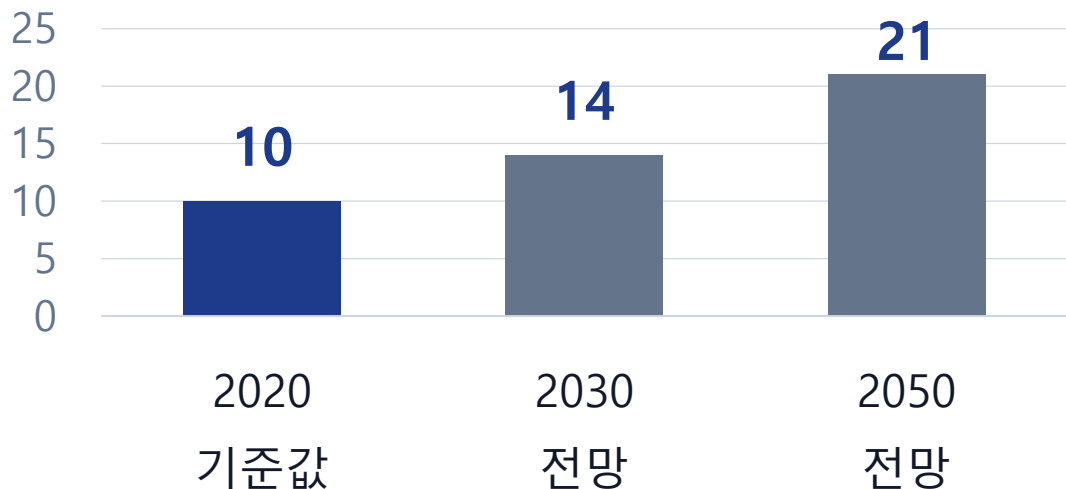
Method와 Evaluation은 실험별로 통합하여 설명합니다.

핵심 정리 p.43 · 참고문헌 p.44–55 · Q&A p.56

가정용 로봇의 역할이 커질 수 있는 사회적 배경

세계 60세 이상 인구

단위: 억 명



한국의 고령 1인가구

2023년 · 가구주 65세 이상

213만 8천 가구

전체 고령자 가구
565만 5천 가구 중 37.8%

1인가구는 외로움·돌봄 필요와
같은 지표가 아님

고령화와 가구구조 변화로 가정 내 지원 기술의 역할을 검토할 필요가 있음

로봇은 후보 중 하나이며, 이 통계가 로봇의 효과를 입증하지는 않음

이 논문은 어떤 로봇을 다루는가?

이 연구에서 사용하는 정의

**센서·액추에이터·이동성을 가진
사이버-물리 시스템(CPS)**

가정이나 주거 환경에서 사용하도록
설계·가격 책정된 로봇

센서	액추에이터	이동성
환경 감지	물리적 작용	환경 내 이동

자율성·인터넷 연결을
필수 조건으로 두지 않음



Figure 1. 왼쪽부터
RoboSapien V2 · Rovio · Spykee

정상적 사용에서 로봇 기능은 어떻게 쓰이는가?

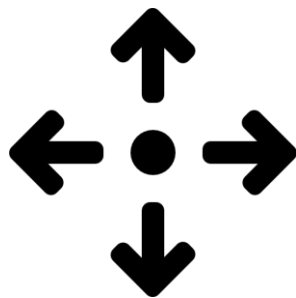
관찰·상태 확인



집 안의 상태를
영상·소리로 확인

원문 기능 예시

필요한 위치로 이동



필요한 곳으로 이동
관찰·상호작용

원문 기능 예시

원격 대화



떨어져 있는 사람과
소리·영상으로 대화

원문 기능 예시

물리적 생활 보조



집안일이나
건강·돌봄을 보조

일반적·미래적 활용

세 실험 로봇이 모두 모든 기능을 갖춘 것은 아님

같은 기능이 악용되면 무엇이 달라지는가?

관찰·상태 확인

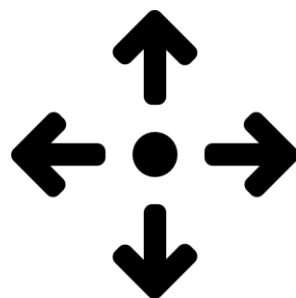


정상: 상태 확인

사생활 관찰

영상·음성에 대한
비인가 접근 시

필요한 위치로 이동



정상: 위치 이동

접근·관찰의
범위 확대

이동 가능한 공간 안에서

원격 대화



정상: 원격 대화

마이크: 도청
스피커: 유해 음성

수음과 재생을 구분

물리적 생활 보조



정상: 물리적 보조

물건·주변 환경에
유해한 간섭

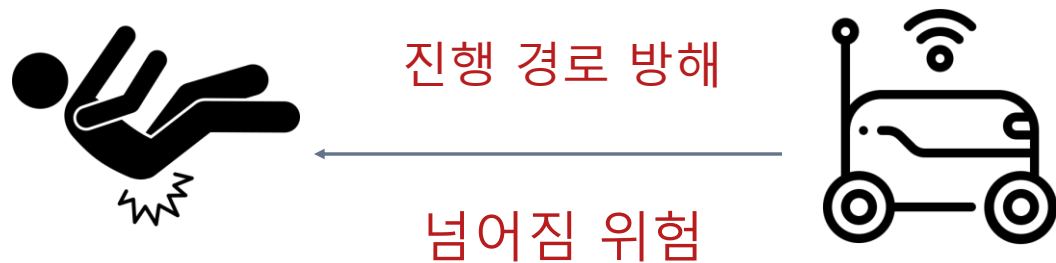
조작 능력과 환경에 따라

기능 자체가 취약점은 아님 · 특정 스트림 노출과 전체 제어권 장악은 구분

돌봄 상황에서는 이용자 조건에 따라 위험이 달라질 수 있다

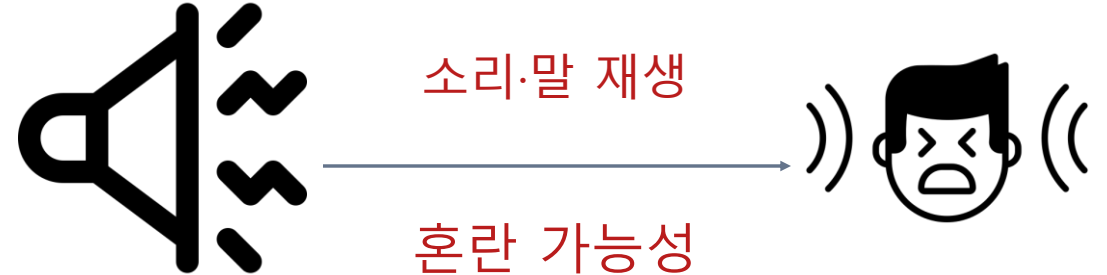
이동 관련 시나리오

이동·균형에 제약이 있고
접근 소리를 알아차리기 어려울 때



음성 관련 시나리오

인지적 어려움이 있는 이용자에게
혼란을 주는 음성을 재생할 때



모든 고령자가 같은 신체·인지 제약을 가진 것은 아님

저자의 잠재적 시나리오 — 실제 사람 대상 피해 실험 아님

가정 환경과 물리적 작용이 만나는 지점

민감한 정보·물건

사적인 대화·영상,
보호할 생활 물건

다양한 이해관계자

사용자뿐 아니라
가족·방문자·반려동물

관리·사용의 제약

전문적인 시스템 관리를
전제하기 어려운 환경

감지 · 이동 · 작동이 실제 생활 공간과 연결

사생활

집 안의 음성·영상 노출

재산

물건·환경의 훼손

신체적 안전

사람의 부상·건강 피해

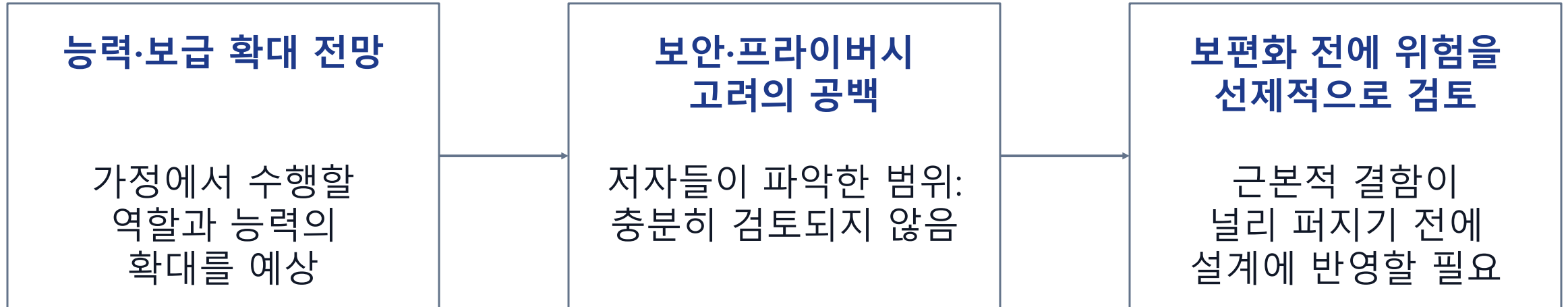
심리적 영향

불안·정서적 피해

영향의 성격은 로봇의 능력, 이용자, 배치 환경에 따라 달라짐

왜 2009년에 이 연구가 필요했는가?

가정용 로봇이 비교적 초기 단계였을 때의 문제의식



관련 연구가 전무했다는 뜻으로 확대하지 않음

그렇다면 저자들은 정확히 무엇을 확인하려 했는가?

저자들은 정확히 무엇을 밝히려 하는가?

당시 상용 가정용 로봇에는 어떤 보안·프라이버시 취약점이 있으며,
어떤 접근 조건에서 공격자가 정보에 접근하거나
로봇의 동작을 이용할 수 있는가?

개별 로봇 또는 여러 로봇·장치의 능력을 함께 고려하면,
가정 내에서 어떤 보안·프라이버시 위험이 가능해지는가?

실제 접근 가능한 정보와 동작을 확인해야
보호할 대상과 조건을 구체화할 수 있음

실험 관찰 —————> 위험 종합·설계 질문

원문 연구 목적을 바탕으로 재구성

어떤 로봇과 어떤 특성을 조사하는가?

당시 상용 가정용 로봇 3종

서로 다른 이동성·조작성·센싱·통신 특성을 대표하도록 3종 선정

Rovio	Spykee	RoboSapien V2
802.11 무선	802.11 무선	적외선

조사 항목을 발표용으로 묶음

장치 식별·통신 노출	정보·기능에 대한 접근	작동 알림·물리 능력
-------------	--------------	-------------

직접 조사: 해당 제품·설정

분석 확장: 개별·결합 상황의 위험과 설계 질문

공격자는 어떤 조건에서 시작하는가?

정보 획득 / 로봇 동작 이용 / 장치 능력 결합

접근 상황	필요한 조건·실험 설정	구분할 점
로컬 무선	무선 범위 + 해당 패킷 관찰·주입 능력	발견 가능성과 내용 접근은 다름
인터넷	서비스 도달 가능 + 필요한 원격 설정	동작 제어의 자격 증명은 별도
중간자	Spykee 클라이언트를 공격 머신에 연결하도록 설정한 실험	그 위치를 얻는 현실적 과정까지 검증한 것은 아님
적외선	리모컨·가시선 또는 리피터를 통한 명령 전달 경로	RovoSapien 자체의 네트워크 침해가 아님

발견 ≠ 정보 접근 ≠ 동작 제어 ≠ 시스템 전체 장악 * 중간자 공격 = MITM(Man-in-the-Middle) 공격

자격 증명은 선행 공격으로 얻을 수도 있음

안전한 무선망·통상적 보안 관행은 많은 공격을 완화할 수 있음

실제 보안은 설정·관리에 의존 · 모든 암호화 우회 주장 아님(WPA2 미실험)

이 연구는 어디까지 확인하려 하는가?

원문 연구 내용과 발표자가 정리한 주장 범위

연구에서 하려는 일	입증했다고 말할 수 없는 범위
선택한 제품에서 정보·기능 접근과 물리 능력을 조사	모든 제품·공격 경로의 전수 조사
실험 결과를 바탕으로 개별·복합 공격 가능성을 분석	모든 신체적·심리적 피해를 실제로 재현
관찰을 종합하여 교훈과 설계 질문을 제안	방어 기법의 효과 검증·안정성 인증

원문 명시: 버퍼 오버플로 등 모든 공격 벡터를 조사하지 않음

이 문제를 기존 연구가 어디까지 다루었는지 살펴보겠습니다

가정 환경의 기술 과제와 안전 인식은 이미 논의되고 있었다

비교 기준	[13] Edwards & Grinter 2001	[34] Young et al. 2008 online / 2009 issue
대상·범위	점진적으로 기술이 추가되는 가정	가정용 로봇 수용·안전 인식 당시 북미 맥락
접근·근거	현장·역사·사례를 종합한 과제 분석	사회심리학 모델을 로봇 사례에 적용
기존 성과	통합·관리·이해 가능성의 설계 과제	통제 가능성·안전 인식의 설계 지침

검증 성격: 사례·문헌 기반 분석 — 실제 공격 실험과 구분

안전·윤리 논의도 선행: 로봇 안전 [8] · 군사 로봇 윤리 [4]

Asimov의 3원칙 [5]과 그 한계 [1, 3, 11]

이 배경의 이해와 특정 로봇의 공격 가능성을 직접 확인하는 것은 다르다

실제 장치의 보안 위험을 확인하는 실증적 접근이 있었다

탐색적 보안 연구의 선례 [2, 16, 17, 20]

대표 사례: Halperin et al. [16], 2008



확인한 것

정보 노출
비인가 동작·설정 변경 가능성

검증 범위

단일 ICD 모델 · 실험실 환경
공격 거리 수 cm

방어 시제품도 제안·평가 · 실제 이식형 장치에 통합한 검증은 아님

실제 장치 분석의 방법론적 선례는 있었지만, 가정용 로봇은 별도의 검증이 필요했다

프라이버시 위험을 설계 질문으로 구체화하는 방법도 있었다

Hong et al. [18], 2004



원문 설명을 바탕으로 재구성한 도식 · 원문 Figure 아님

적용: 위치 기반 메신저 · BEARS 긴급 대응 서비스
인터뷰·저충실도 프로토타입 활용

보안 위협 모델과 병행할 필요가 있음

Spotlight는 질문 구성 방식을 참고하여
로봇의 기능·사람·환경·장치 결합에 관한 질문을 제안

그렇다면 가정용 로봇에서 무엇을 추가로 확인해야 하는가?

기존 성과	Spotlight에서 추가로 확인할 질문
가정 기술의 통합·관리 문제 이해	해당 로봇에서 어떤 정보와 기능이 노출되는가?
로봇의 수용·안전·윤리 논의	악의적 개입 아래 누가 어떤 기능을 이용할 수 있는가?
실제 장치의 보안 분석 접근	통신·감지·이동·조작 능력은 어떤 조건에서 이용되는가?
프라이버시 위험을 구조화하는 설계 방법	실험 관찰과 장치 결합을 어떤 설계 질문으로 연결할 것인가?

선행연구의 관점 위에서, 실제 가정용 로봇의 접근 조건과 공격 가능성을 실험으로 확인

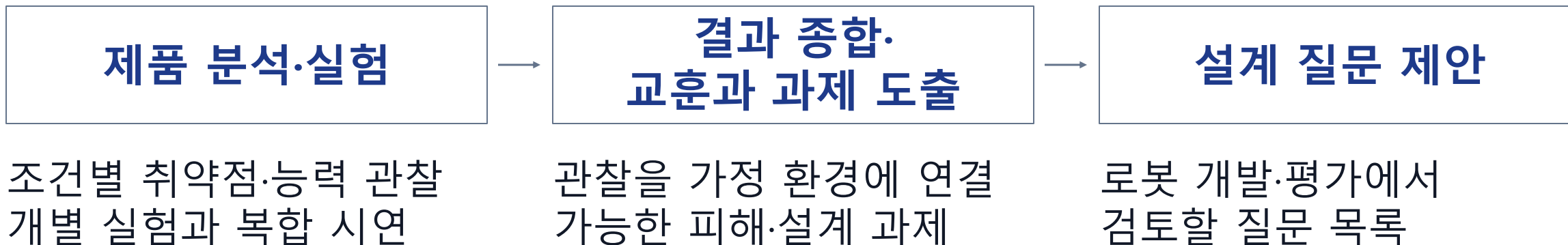
선행연구를 부정한 것이 아니라, 가정용 로봇에 대한 적대적·실증적 검증을 추가

기존 보안 관행·안전한 무선망도 많은 공격을 완화할 수 있음

다음: 저자들은 어떤 로봇을 선정하고, 어떻게 분석했는가?

실험에서 설계 질문까지: 무엇을 어떻게 알아내는가?

출발점: 당시 상용 로봇의 기능·통신 방식과 접근 조건



각 단계의 근거를 구분: 실험 관찰 / 위험 시나리오 / 설계 제안

탐색적 연구의 산출물이며, 완성된 방어 시스템의 효과 검증은 포함하지 않는다

서로 다른 능력의 로봇을 왜 선택했는가?



Figure 1. 왼쪽부터
RoboSapien V2 · Rovio · Spykee

3종·확보 4개체 / 시험별 반복수 미기재 / 특정 버전의 관찰

대상	제어·통신	영상·음성 / 집기
Rovio	웹 UI 802.11	AV 제공 집기 불가
Spykee	PC 콘솔 802.11	AV 제공 집기 불가
RoboSapien V2	리모컨 적외선	AV 미제공 집기 가능

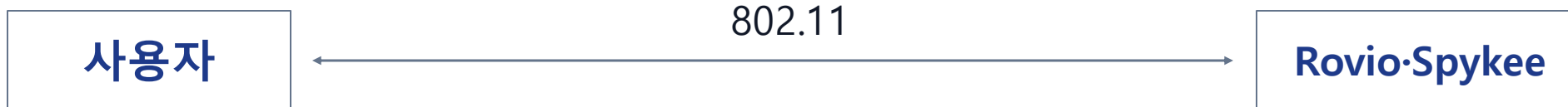
이동·조작·감지·통신의
차이를 함께 살펴보기 위한 선정

AV = 사용자 영상·음성 스트림
RoboSapien의 내장 카메라와 구분

사용자와 로봇은 어떻게 연결되는가?

802.11: 무선 연결 방식 · AP: 무선 단말의 접속점 · 콘솔: 제어 프로그램

Ad hoc
AP 없이 직접



로컬 연결
같은 가정망



원격 연결
인터넷 경유



Rovio: 포트 전달 설정 · Spykee: 도달 가능한 호스트명 또는 등록·원격 허용

명령은 사용자에서 로봇으로, 영상·음성은 반대 방향으로 전달

적외선(IR)



로봇이 있다는 사실을 어떻게 알아냈는가?

SSID = 무선망 이름 / MAC 주소 = 네트워크 장치를 구분하는 주소

필요한 위치·접근	관찰·질의 단서	저자가 보고한 식별 근거
무선 범위에서 패킷 관찰·주입	Ad hoc의 SSID Infrastructure의 MAC 주소	제품을 구별하는 이름·주소 특성
서비스에 도달하여 응답 질의	Rovio: 포트 80 Spykee: TCP 9001	제품 특유의 응답
등록된 원격 연결의 관련 트래픽 관찰	Spykee의 주기적 keep-alive (연결·등록 유지 패킷)	spykeeworld.com으로 보내는 식별 단서

저자 추정: 검색 엔진으로 Rovio를 찾을 가능성
검색 실험·발견률을 보고한 결과와 구분

발견 가능성 ≠ 통신 내용 해독 ≠ 동작 제어

로그인 정보와 영상은 어떻게 노출되는가?

인코딩

표현 형식 변환
Base64 자체는 기밀성 없음

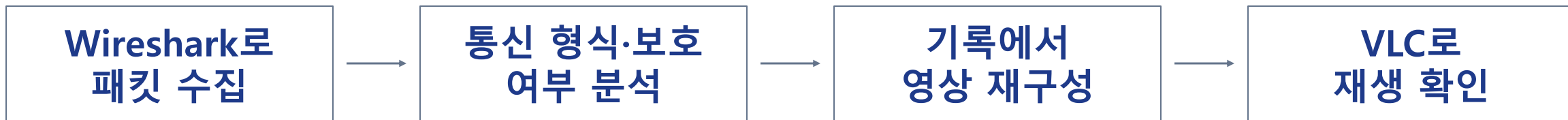
암호화

키를 이용해
내용을 읽기 어렵게 보호

인증

주장하는 신원이
맞는지 확인

전제: 로봇과 사용자의 해당 트래픽을 관찰할 수 있는 위치

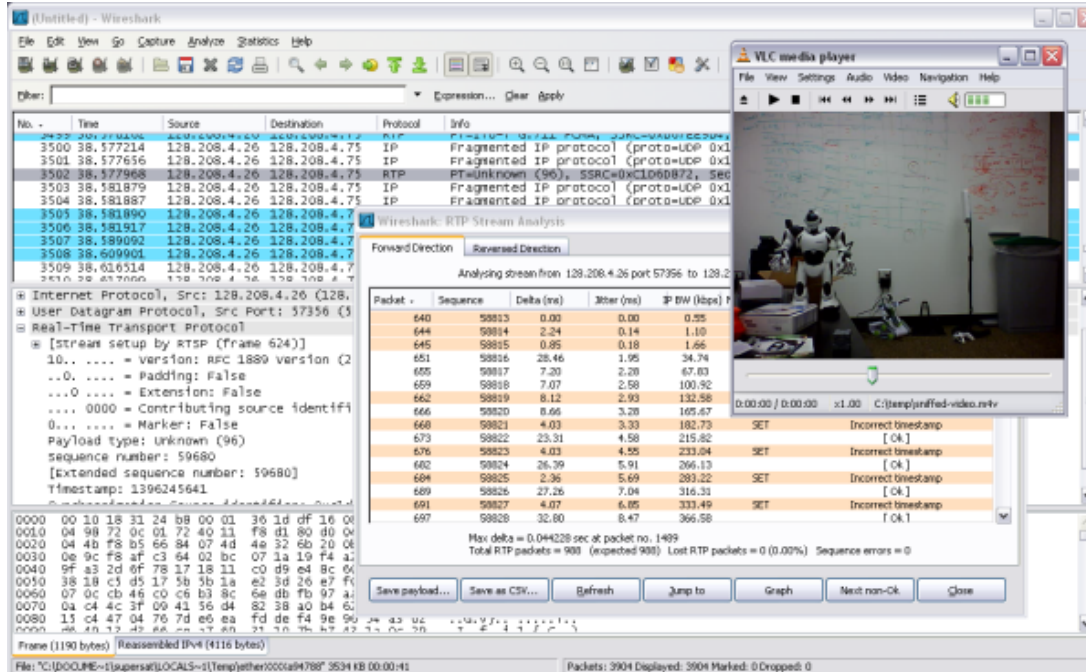


RTSP는 스트림의 설정·제어 / MPEG4·MJPEG는 원문에 나온 영상 형식

Wireshark·VLC는 기존 도구

저자들은 해당 로봇의 트래픽을 분석하고 영상 복원을 확인

실제로 무엇을 복원했고 어떤 조건이 필요했는가?



Rovio : Ad hoc / 로컬 / 인터넷 원격

자격 증명·영상·음성 비암호화
영상 재구성·재생 확인

Spykee : Ad hoc / 로컬

자격 증명 평문·MJPEG 비암호화
영상 재구성·재생 확인

Spykee : 원격

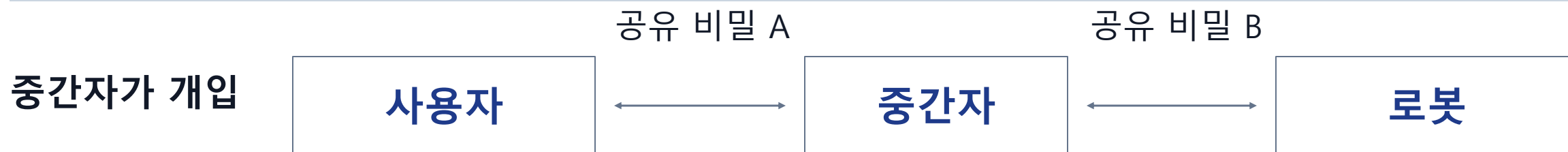
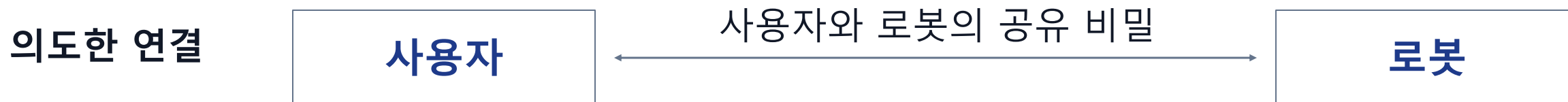
DH 키 교환 사용
별도 중간자 실험으로 확인

Figure 2. Rovio 영상 복원의 제시 화면
조건: 해당 트래픽에 접근하여 기록을 수집

별도 경로: Rovio는 웹 비밀번호를 설정해도, 도달 가능한 RTSP 스트림에 인증 없이 접근

키 교환이 있는데도 왜 중간자가 개입할 수 있는가?

Diffie-Hellman(DH): 두 당사자가 공유 비밀을 합의하는 키 교환



중간자는 양쪽과 각각 공유 비밀을 합의
통신 상대가 누구인지 확인하는 절차가 필요

키를 합의했다는 사실만으로 상대의 신원이 보장되지 않는다

개념 설명용 재구성 · Spykee의 실제 패킷·암호 파라미터를 나타내지 않음

Spykee 중간자 실험은 어디까지 입증했는가?

실험 설정: Spykee 콘솔이 공격 머신의 호스트명으로
직접 연결하도록 구성



공격 머신이 Spykee에 별도로 연결하고, 사용자와 로봇 양쪽의 DH 키 교환을 각각 수행

저자 보고

새 원격 연결에 필요한 로그인 자격 증명 추출
해당 세션의 영상·음성 복원 가능

이 실험이 답하지 않은 것

현장에서 중간자 위치를 얻는 과정
성공률·소요시간·거리의 일반화

제어 권한과 사용자 알림은 어떻게 달랐는가?

Rovio·Spykee 동작 제어: 유효한 자격 증명 + 연결 가능 조건
원격 제어는 로봇이 외부에서 접속 가능하도록 설정된 경우에만 가능

관찰 항목	Rovio	Spykee
로그인 알림	소리 없음 시각적 단서 제한적	차임 소리 있음 즉시 음량을 낮춰 효과 약화 가능
도킹 중 영상·음성	전원이 켜져 있으면 전송 가능	도킹 중에는 전송하지 않음
이동 소음	이동 소음이 뚜렷함	이동 소음이 뚜렷함

RoboSapien V2: 적외선 제어 / 보행 소음과 간헐적 음성

관찰된 알림 특성으로 사용자 인지율·반응시간·경고 효과를 정량화할 수는 없다

제어 가능한 로봇은 실제로 무엇을 할 수 있는가?

RoboSapien V2의 물리 능력 조사

시험·특성	원문 관찰
도달 범위	바닥과 바닥 위 약 50 cm
들기	열쇠 집기·250 g 물체 들기
문 열기	손잡이는 잡았으나 열지 못함 저자 설명: 파지력 부족
성냥 점화	성공하지 못함 정밀한 조작에 어려움

손 내부 폭: 닫힘 약 1.5 cm / 열림 약 7.5 cm
들기에 여러 시도 필요 · 세 로봇 모두 가벼운 물체 밀기 가능
관찰 수치이며 최대 정격 하중·작업별 성공률을 측정한 결과는 아니다

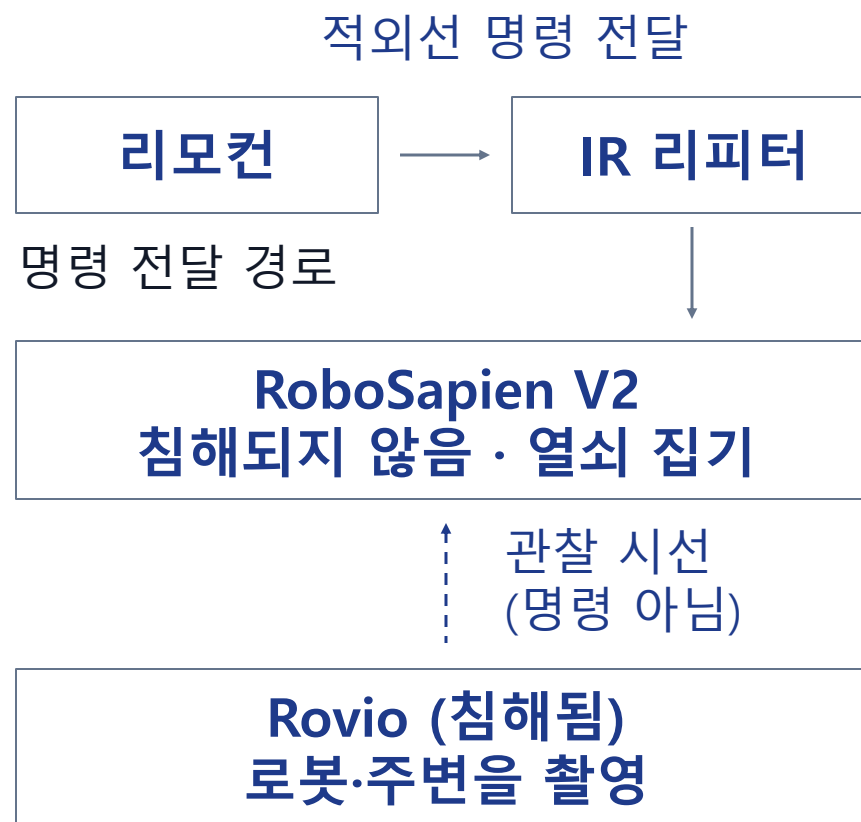


외형 참고 (선택)
볼링 핀 사진 · 하중 시험 아님

두 로봇의 능력을 어떻게 결합했는가?



Figure 3. RoboSapien이 Rovio 앞에서 열쇠를 든 모습
리모컨·리피터의 역할은 오른쪽 설명 도식에서 구분



공격자가 장치를 조정
로봇 간 자율 협업을 구현한 실험 아님

결합 실험의 결과는 어디에서 끝났는가?

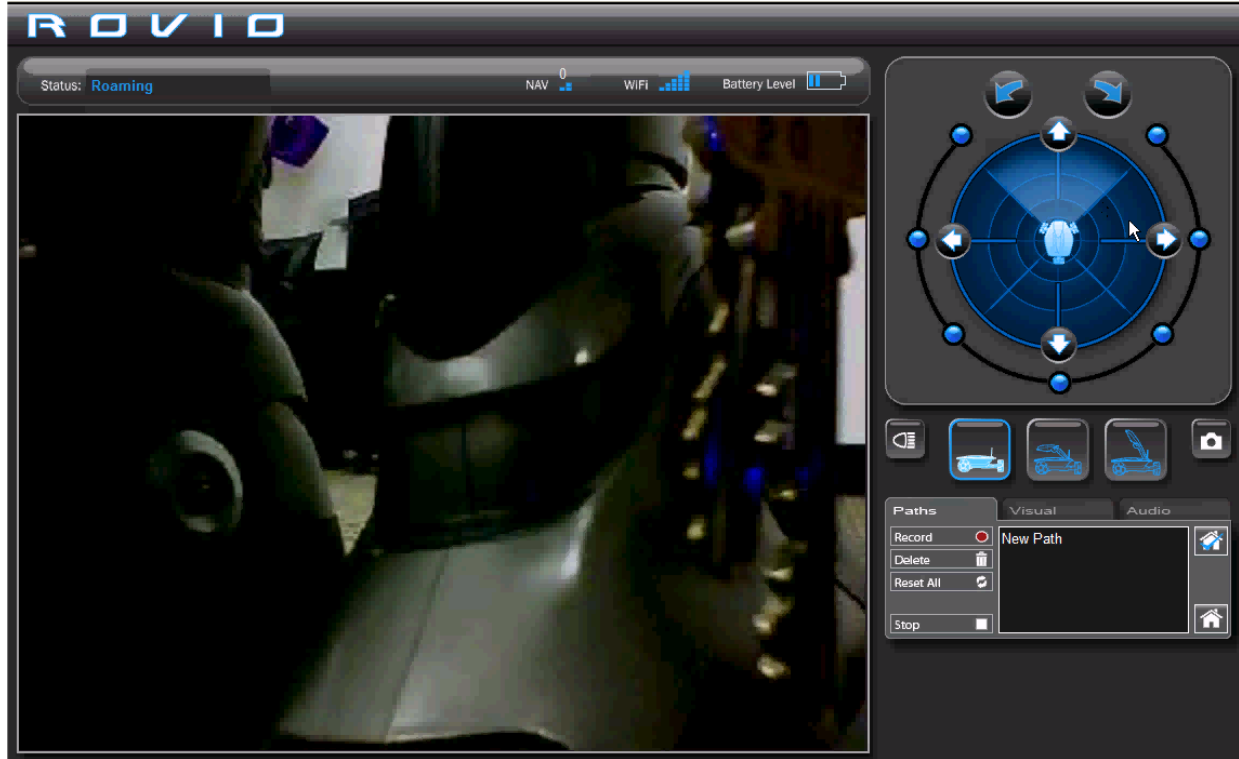


Figure 4. Figure 3과 같은 시험의 Rovio 영상
전체 인터페이스를 본 뒤 영상 속 열쇠 위치를 확인

실험실에서 시연한 것

열쇠를 집어 위치 조정
Rovio로 열쇠 영상 확보

실제 열쇠 제작은 미수행

사진 기반 복제 [21]와 연결
복제품 제작·잠금 해제까지
검증하지 않음

다양한 집·열쇠·조명·배치에서의 성공
률과 소요시간은 제시하지 않음

실험 관찰을 가정의 위험으로 어떻게 확장했는가?

출발한 관찰	저자가 논의한 위험 시나리오	근거의 성격·경계
영상·음성 접근	가정과 아동의 사생활 침해 가능성	접근 실험에서 피해 가능성을 논의 실제 피해 확률은 측정하지 않음
이동·물체 조작	재산·로봇 자체 손상 환경을 이용한 신체 위험	물리 능력 관찰 + 피해 시나리오 돌봄 상황의 실제 위해 실험 아님
알림·음성 상호작용	사용자 인지의 어려움 심리적 피해 가능성	알림 관찰 + 인용 선행 연구 정서적 유대 [19,27] 등은 간접 근거

사용자 외에도 방문자·아동·고령자·장애인·반려동물이 영향을 받을 수 있음

설계자는 사용자의 기대·이해 방식과 보안 설정·교육의 어려움도 고려해야 함

가능한 위험의 예시이며, 모든 피해를 재현하거나 심각도·발생 빈도를 산정한 목록은 아님

설계 질문은 무엇을 묻고, 효과까지 검증했는가?

실험·위험 논의를 로봇 개발과 평가에서 검토할 질문으로 정리

사회·환경·기술적 속성

Social, Environmental, and Technical Questions

기능·이동·조작·감지·통신
사용자·주변 사람과 동물·운용 환경
개발 과정·외부 부품·업데이트

보안·프라이버시 위험

Security and Privacy Questions

사생활 침해 / 재산·물리적 무결성
신체 안전·심리적 피해
다른 로봇·기술과 결합한 공격

예: 감지·이동 능력이 있는 로봇이 사적 공간의 어떤 정보를 노출할 수 있는가?

질문을 제안했으나, 적용 전후의 위험 감소 효과는 검증하지 않았다

지표·최소 기준·소비자 평가·감독도 제안 단계 · 완성된 인증 체계를 구현한 결과는 아님

전체 증거로 무엇을 말할 수 있는가?

말할 수 있는 주장	논문이 제시한 증거	이 증거로 확정할 수 없는 것
조건별 정보·기능 노출	통신·제어 실험 보고 Fig.2 / Tables 2·3	전체 제품 취약률 실제 가정 환경에서의 공격 성공률
능력 결합으로 새로운 공격 가능	열쇠 집기·촬영 시연 Figs.3·4	실제 열쇠 제작·잠금 해제 다양한 환경에서의 성능
사람·환경도 고려 필요	알림·물리 관찰 시나리오·선행 연구	사용자 인지율 피해 확률·심각도
설계·평가 질문 제공	관찰을 종합한 질문 목록	질문 적용 전후의 보안 개선 효과 목록의 완전성

특정 제품·버전·접근 조건의 결과 / 시험별 반복 분포 미기재

모든 공격 경로·버퍼 오버플로는 미조사 / WPA2 미실험 / Rovio WPA 업데이트 미적용

저자도 통상적 보안 관행·안전한 무선망이 많은 공격을 완화할 수 있음을 인정

이 논문은 어떤 지식과 관점을 제공했는가?

실제 제품에서 확인한 취약점

실증은 실제 관찰·실험에서 얻은 근거
선택 제품의 정보·동작 접근을 조건별 확인

제품 분석·영상/제어
Tables 1–3, pp.3–5

결합·생활 환경의 위험 관점

보완적인 능력의 결합을 시연하고
사람·환경을 고려하는 논의로 확장

복합 시연, p.7
사람·환경, pp.7–8

설계 질문 제안

설계 때 확인할 특성과 위험을 묻는 질문
기능·사용 환경을 위험 검토와 연결

Design Questions
두 묶음, pp.8–9

능력: 로봇으로 얻을 수 있는 정보와 수행할 수 있는 행동

Rovio의 원격 관찰 + RoboSapien의 물체 조작을 함께 이용해 열쇠 집기·촬영

침해된 Rovio + 침해되지 않은 RoboSapien / 명령 전달: 리모컨·적외선 리피터

실험적 관찰 / 확장 논의 / 설계 제안은 증거 성격이 다름

개별 제품의 분석을 장치 결합과 생활 환경의 보안 검토로 연결했다.

기존 기술의 활용과 이 논문의 기여를 구분한다

이 논문의 기여로 볼 수 없는 것	이 논문의 실제 범위
Wireshark·VLC, Diffie-Hellman·MITM 개념의 발명	기존 수단으로 해당 제품의 구현·접근 조건을 분석
열쇠 복제 기술 개발 복제 열쇠 완성	[21]에 연결되는 집기·촬영 시연 실제 복제 열쇠는 미제작
질문 기반 설계의 최초 제안 방어 효과의 입증	Hong [18]과 유사한 질문 구성 로봇별 질문 제안, 방어 효과 미검증
전체 로봇의 위험도 모든 신체·심리 피해의 입증	선택한 제품의 실험 잠재적 영향에 관한 논의

도구는 연구를 수행한 수단이고,
기여는 그 사용으로 추가된 발견·지식·관점이다.

기존 도구를 사용했어도, 그 도구로 새롭게 확인한 지식에는 기여가 있다.

한계를 고려해도 어떤 가치가 남는가?

일반화: 관찰한 제품·조건의 결과를 다른 대상·상황에 적용하는 것
특정 조건의 관찰과 시장 전체의 빈도·효과 측정은 다르다.

평가 관점	근거가 있는 가치	확대하면 안 되는 결론
실증적 지식	특정 조건에서 정보 노출과 기능 접근을 확인	모든 제품의 취약률 시장 전체의 취약률·실제 환경의 공격 성공률
위험을 보는 관점	장치 결합·생활 환경을 검토할 문제로 구체화	모든 장치 조합의 위험 / 실제 피해 확률·심각도
설계 제안	설계자가 검토할 질문의 출발점	완전한 목록·검증된 방어 안전 보증

실제 사례로 문제·검토 과제를 구체화한 탐색적 연구로서 가치가 있다.
제품 실증을 장치 결합·생활 환경·설계 질문으로 연결했다.

저자도 통상적 보안 관행이 많은 공격을 완화할 수 있음을 인정한다.

이 논문은 무엇을 다음 과제로 남겼는가?

원문의 논의를 세 축으로 재구성

평가 기준과 소비자 정보

무엇을 측정하고
어떤 기준을 알릴까?

평가 지표·최소 기준
소비자가 판단할 정보

사용자와 생활 환경

누가 상태와 위험을
어떻게 이해할까?

사용자의 기대와 실제 동작
환경·접근성에 맞는 알림

여러 로봇과 장치의 결합

함께 사용하면
무엇이 가능해질까?

개별 기능이 합쳐질 때의
정보 획득·물리 조작

평가 지표: 측정할 것

최소 기준: 만족해야 할 조건

멘탈 모델 = 사용자가 기대하는 작동 방식

로봇청소기 조사에서는 무엇을 어떻게 점검했는가?

한국소비자원·KISA / 6개 제품 / 조사 2025.03.03~07.31 / 보도 2025.09.02

모바일앱

정책 관리

기기

16 + **3** + **21** = **40개 점검 항목**

점검 항목 = 확인할 대상·조건 / 40개는 취약점 수가 아님

네트워크: 6개 제품 모두 양호

안전한 통신 프로토콜 사용 등

네트워크가 양호해도 앱 권한과 펌웨어는 별도 문제

일부 앱의 접근제어 문제, 펌웨어의 취약 설정 등

조치완료: 특정 사항의 수정 완료 보고

개선계획: 앞으로 이행할 계획

주요 사진·카메라 사례는 보도 당시 조치완료 / 모든 개선 권고의 완료를 뜻하지 않음

ETSI EN 303 645: 소비자 IoT 기본 요구사항 / 기준의 존재와 제품의 안전 보증은 구별

암호화되어 있어도 사진·카메라 접근 권한은 별도로 확인해야 한다

나르왈: 암호화된 사진과 키 접근

별도 인증 없이 사진 URL에 접근
클라우드에서 사용자 "개인키" 취득
사진 복호화·열람 가능

자료 암호화와 복호화 키의 접근 보호는 별개

드리미: 일부 권한을 공유받은 사용자

청소·지도 작성 권한을 공유받은 조건에서
허용 범위 밖의 카메라 기능에 접근



기관 설명 도식 / 일부 권한을 공유받은 조건

인증: 요청자의 신원을 확인

인가: 해당 기능·자료의 사용 권한을 확인

두 사례 모두 보도자료상 조치완료(2025) / 2026년 현재 제품 상태는 미확인

로봇의 프라이버시 상태 전달은 어디까지 검증되었는가?

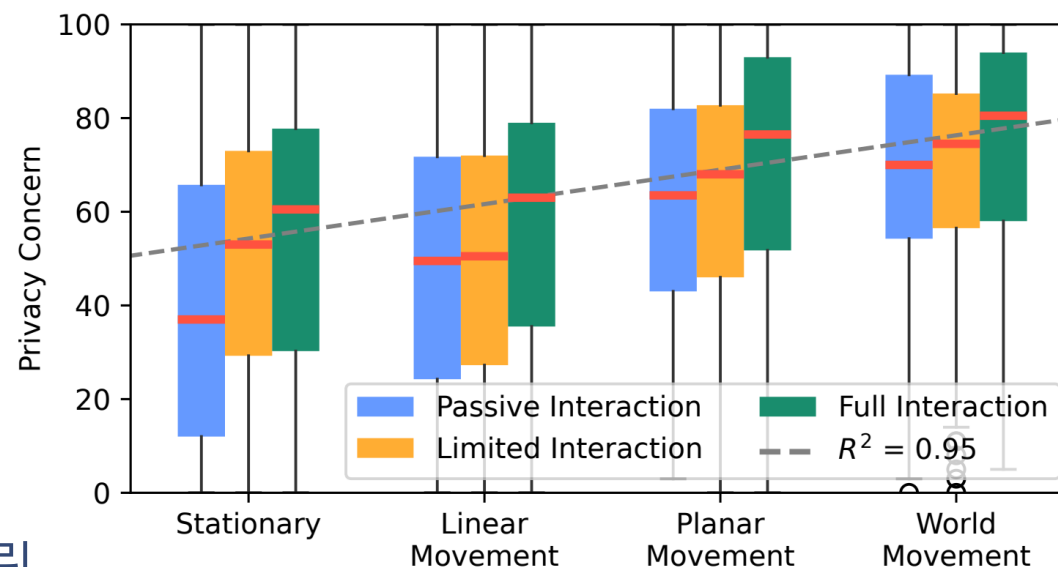
Privacy Communication Patterns for Domestic Robots

- I 온라인 N=90
로봇 특성과 프라이버시 우려
- II 포커스 그룹 N=22
상태 전달·개입 패턴 86개 구성
- III 온라인 N=1,720
이해·신뢰·선호 등 평가

상태 전달: 현재 센서·연결 상태를 사용자에게 알림

개입: 카메라 차단처럼 기능 자체에 직접 개입

Study I · N=90 · 프라이버시 우려 응답(0-100)
공격 성공률·침해율을 측정한 그림이 아님



사용자 평가의 진전 / 기술 구현·침해 시 상태 정확성 검증은 별도

제안 1: 표시·권한·실제 센서 동작이 일치하는가?

센서 “꺼짐” 표시만으로 기존 저장 자료의 접근·삭제 상태까지 알 수 있을까?

사용자에게 보이는 상태

실제 센서·데이터 경로



권한별로 대조 / 독립 관찰과 로컬 차단을 단계적으로 적용

조건: 허가된 기기·계정·서버와 시험 데이터 / 제한 계정·앱 침해 조건을 분리

신뢰 경계: 보호할 부분과 침해 가정 부분의 경계 / 독립 관찰 경로는 보호된다고 가정

회귀시험: 업데이트 후 같은 조건을 다시 확인

측정 후보

권한 밖 허용률·표시 불일치 횟수/시간
차단 지연·차단 후 시험 데이터 전송량

사용자의 상태 이해 정답률
정상 작업의 잘못된 차단 비율

제안 2: 여러 장치의 결합 위험을 어떻게 검사할 것인가?

결합 상황 평가: 장치를 함께 이용할 때의 허용 범위를 검사

단일 장치

장치 결합

결합 + 제약 적용



각 장치에서 가능한
정보 획득·물체 이동

같은 조건에서 단일 / 결합 /
제약 적용을 비교

권한·동작 범위를 제한하고
위험과 정상 기능을 재비교

사람의 관찰과 원격 명령을 통한 결합도 포함 / 로봇 간 직접 통신은 필수 조건이 아님

공통 조건: 권한·제어 경로·시험 물체·조명·초기 상태 / 안전한 제한 공간에서 반복

권한 밖 정보·물체 이동과 반복성을 확인하고, 정상 작업 완료율·잘못된 차단도 비교

제안 3: 설계 질문이 실제 검토를 개선하는가?

같은 설계 사례·검토 과제

기준 조건	비교 조건
일반 보안 점검 자료	일반 자료 + 로봇 특화 설계 질문
공통 통제: 같은 위험 사례·채점 규칙 사용 시간·자료량·참여자 경험을 두 조건에서 맞춤	
대조 조건 = 비교의 기준이 되는 상황 / 조건을 모르는 평가자가 동일 규칙으로 채점	
측정 후보	준비한 위험 사례 발견 비율 근거 없는 위험 판정 비율
	검토 소요 시간 평가자 간 일치도
평가자 간 일치도 = 같은 사례에 대한 판단의 일치 정도	
문항 수 증가와 품질 개선은 다름 / 추가로 발견한 타당한 위험은 별도 평가	
실제 상태·장치 결합·설계 검토의 효과를 조건과 지표로 확인한다	

이 발표에서 가져갈 세 가지

01 실제 제품에서 확인한 접근 조건

특정 버전·접근 조건에서 정보 노출과 동작 이용을 보고했다.
장치 발견, 정보 접근, 동작 제어는 서로 다른 조건과 권한을 요구한다.

02 장치의 기능과 생활 환경을 함께 고려

열쇠 집기·촬영의 복합 시연과 사람·환경의 논의를 제시했다.
발표자 평가: 개별 기능의 분석과 결합 상황의 검토가 함께 필요하다.

03 후속 자료를 구체적인 검증 질문으로 연결

2025년 조사는 제품 보안 점검이 구체화됐음을, 2024년 연구는 로봇 상태 전달에 대한 사용자 평가가 구체화됐음을 보여줌

하지만 상태·권한·실제 동작의 일치, 장치 결합 위험, 설계 질문의 효과는 추가 검증이 필요

관찰한 증거의 범위를 지키며, 다음 검증의 조건과 지표를 명확히 한다.

참고문헌 · 리뷰 대상과 사회적 배경

[P0] 리뷰 대상 / 숫자 인용: 원 논문의 참고문헌 번호
문자 ID: 발표 보충 자료 (원문 번호와 별도)

[P0] A Spotlight on Security and Privacy Risks with Future Household Robots:
Attacks and Lessons
T. Denning et al. · UbiComp 2009, pp.105–114

EXT-MOT-01 Ageing and health

WHO · Fact sheet · 2025-10-01

EXT-MOT-02 2024 고령자 통계 · 혼자 사는 고령자의 생활과 의식

통계청 · 2024-09-26 · 사용 위치: PDF p.8 / 인쇄 p.2

참고문헌 · 가정 기술과 로봇 수용

[13]
EXT-REL-13

At Home with Ubiquitous Computing: Seven Challenges

W. Keith Edwards, Rebecca E. Grinter · UbiComp 2001, pp.256–272

[34]
EXT-REL-34

Toward Acceptable Domestic Robots:
Applying Insights from Social Psychology

James E. Young et al. · International Journal of Social Robotics 1, 95–108
온라인 공개 2008-11-18 / 권호 2009년 (P0는 2008년으로 인용)

참고문헌 · 보안 분석과 프라이버시 설계

[16]
EXT-REL-16

Pacemakers and Implantable Cardiac Defibrillators:
Software Radio Attacks and Zero-Power Defenses
Daniel Halperin et al. · IEEE Symposium on Security and Privacy, 2008

[18]
EXT-REL-18

Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing
Systems
Jason I. Hong, Jennifer D. Ng, Scott Lederer, James A. Landay · DIS 2004

참고문헌 · 탐색적 보안 연구의 선례

[2] Tamper Resistance – a Cautionary Note

Ross Anderson, Markus Kuhn · 2nd USENIX Workshop on Electronic Commerce, 1996

[17] Vulnerabilities in First-Generation RFID-enabled Credit Cards

T. S. Heydt-Benjamin et al. · Financial Cryptography and Data Security, 2007

[20] Analysis of an Electronic Voting System

T. Kohno, A. Stubblefield, A. Rubin, D. Wallach · IEEE S&P, 2004

참고문헌 · 안전과 윤리 논의 (1)

- [1] Ethical Guidelines for AI in Education: Starting a Conversation
R. Aiken, R. Epstein · International Journal of AI in Education 11, 2000
-
- [3] Asimov's "Three Laws of Robotics" and Machine Metaethics
S. Anderson · AI & Society 22(4), 2008
-
- [4] Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture
R. Arkin · 3rd International Conference on Human-Robot Interaction, 2008

참고문헌 · 안전과 윤리 논의 (2)

[5] I, Robot

Isaac Asimov · Gnome Press, 1950

[8] Robot Safety

M. C. Bonney, Y. F. Yong (eds.) · IFS (Publications), 1985

[11] Asimov's Laws of Robotics: Implications for Information Technology, Parts 1 and 2

Roger Clarke · IEEE Computer 26(12), 1993 / 27(1), 1994

참고문헌 · 통신 보호와 물리적 열쇠

- [14] Weaknesses in the Key Schedule Algorithm of RC4
S. Fluhrer, I. Mantin, A. Shamir · Selected Areas in Cryptography, 2001
-
- [26] Using the Fluhrer, Mantin, and Shamir Attack to Break WEP
A. Stubblefield, J. Ioannidis, A. Rubin · NDSS, 2002
-
- [21] Reconsidering Physical Key Secrecy: Teleduplication via Optical Decoding
Benjamin Laxton, Kai Wang, Stefan Savage · ACM CCS, 2008

참고문헌 · 사람과 생활 환경

- [19] Designing a Sociable Robot System for Weight Maintenance
C. Kidd, C. Breazeal · IEEE Consumer Communications and Networking Conference, 2006
-
- [22] Affect Recognition in Robot Assisted Rehabilitation of Children with Autism Spectrum Disorder
C. Liu, K. Conn, N. Sarkar, W. Stone · IEEE ICRA, 2006
-
- [27] "My Roomba Is Rambo": Intimate Home Appliances
J. Sung, L. Guo, R. Grinter, H. Christensen · UbiComp 2007

참고문헌 · 상호작용 지표와 사용성

[25] Common Metrics for Human-Robot Interaction

A. Steinfeld et al. · ACM SIGCHI/SIGART Human-Robot Interaction, 2006

[32] Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

A. Whitten, J. D. Tygar · 8th USENIX Security Symposium, 1999

참고문헌 · 네트워크·보안 용어

EXT-ME-NET NIST CSRC Glossary: Ad Hoc Network / Access Point

NIST · 웹 용어 항목 · 발행연도 별도 표시 없음

EXT-ME-ID NIST CSRC Glossary: Service Set Identifier
NIST 정의

NIST · 웹 용어 항목 · 발행연도 별도 표시 없음

EXT-ME-SEC NIST CSRC Glossary: Authentication / Encryption

NIST · 웹 용어 항목 · 발행연도 별도 표시 없음

참고문헌 · 기술 개념의 표준 문서

EXT-ME-ID RFC 7042	IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters D. Eastlake 3rd, J. Abley · RFC 7042 · 2013-10
EXT-ME-B64	The Base16, Base32, and Base64 Data Encodings S. Josefsson · RFC 4648 · 2006-10
EXT-ME-RTSP	Real Time Streaming Protocol (RTSP) H. Schulzrinne, A. Rao, R. Lanphier · RFC 2326 · 1998-04
EXT-ME-DH	Diffie-Hellman Key Agreement Method E. Rescorla · RFC 2631 · 1999-06

참고문헌 · 후속 연구·제품 조사·기준

[SOUPS24]
EXT-FUT-
SOUPS

Privacy Communication Patterns for Domestic Robots

Maximiliane Windl et al. · SOUPS 2024, pp.121–138

[KISA25]
EXT-FUT-KCA

일부 로봇청소기, 카메라 사진 열람 등 보안 취약점 발견돼

한국소비자원·KISA · 보도자료와 붙임 1~5, 13쪽 · 2025-09-02

[ETSI24]
EXT-FUT-ETSI

CYBER; Cyber Security for Consumer Internet of Things:
Baseline Requirements

ETSI EN 303 645 V3.1.3 · 2024-09

감사합니다

Questions & Discussion

안명균
기계공학과 DRCL