ACM WiSec 2024 Trip Report

Koreana Hotel / Korea

개요

2024년 5월에 무선 및 모바일 네트워크의 보안 및 개인정보보호에 관한 컨퍼런스인 WiSec에 참석했다. 해당 학회는 특히 keynote가 인상적이었다. Tesla 루팅에도 성공한 Jean-Pierre Seifert이 양자 내성 암호와 통신보안을 주제로 keynote에서 발표했다. 해 이 외에도 다양한 네트워크 및 네트워크보안 관련 주제들에 대한 심도 있는 keynote와 함께, 여러 연구자의 연구를 들어볼 좋은 기회를 제공해줬다.

Keynote

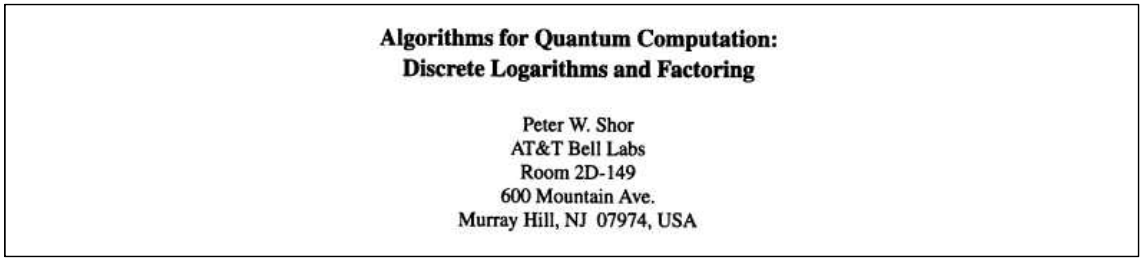
Keynote 1: Quantum Computing and TelCo Security

Jean-Pierre Seifert, TU Berlin, Germany (May 27)

양자 컴퓨팅(QC)의 발전은 기존 컴퓨팅 방식에 비해 엄청난 계산 시간 단축 가능성을 제시한다. QC는 문제의 크기가 커져도 특정 시간에 수렴하는 컴퓨팅 시간을 가지는 것을 가능하게 함으로써, 전통적인 병렬 컴퓨팅의 선형 시간 증가와 차별화된다. Grover의 알고리즘은 양자 컴퓨팅이 어떻게 특정 문제에 대해 기존 알고리즘보다 더 빠른 속도를 낼 수 있는지를 구체적으로 보여주는 예시이다. Grover의 알고리즘은 무작위 탐색 문제에서 기존의 알고리즘보다 제곱근 시간 안에 결과를 도출할 수 있어, 양자 컴퓨터가 충분한 큐빗을 갖추고 있으면 실질적인 보안 위협이 될 수 있다. 이 발표에서는 이러한 QC의 특징을 기반으로 Grover's attack이 가능하다는 것을 주장했다. 특히, Grover의 공격을 구현하기 위해서는 최소 256개의 큐빗을 갖춘 양자 컴퓨터가 필요하다고 이야기했다.

또한, 3G부터 사용된 Authentication and Key Agreement(AKA) 보안 프로토콜을 PQC로 바꿀 필요가 있음을 주장했다. AKA 프로토콜은 다양한 암호화 알고리즘을 혼합하여 사용함으로써 단일 알고리즘의 취약점을 통한 공격을 어렵게 만들지만, AES 계열 알고리즘의 사용은 문제점으로 지적했다. 이에 따라, 5G 네트워크에서는 더욱 안전한 Post-Quantum Cryptography(PQC)로의 전환을 제안했다.

이 발표는 Grover's Attack과 같이 양자 알고리즘을 이용하여 유사한 연산 패턴을 가진 알고리즘들을 공격하는 방법에 대한 이해를 제공했으며, QC가 현대 보안 체계에 미치는 영향을 이해하는 데 중요한 배경지식을 제공해줬다. 그러나 QC를 이용한 암호공격의 실험적 증거나 실제 적용 사례가 아직 부족한 것으로 알고 있는데, 제안한 기법이 실용성이 있을지 의문이다.



Algorithms for Quantum Computation:
Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Vision Talk

Vision Talk : Security & Privacy Issues of Electric Vehicles and Batteries

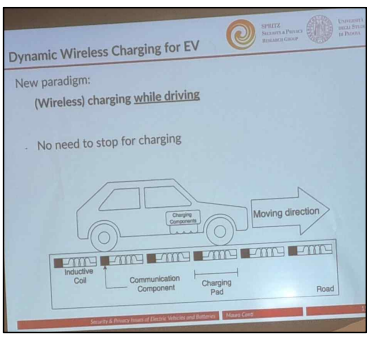
Wenyuan Xu, Zhejiang University, China (May 27)

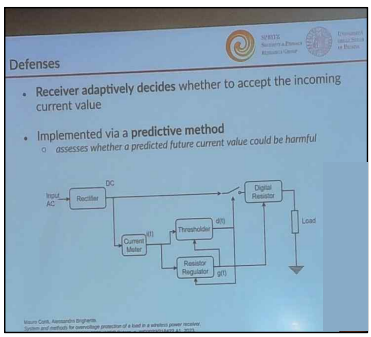
최근의 기술적 진보는 자동차를 복잡한 컴퓨팅 및 통신 시스템으로 변화시켰다. 이 발표에서는 전기 자동차(EV) 및 동적 무선 전력 전송(DWPT) 기술과 관련된 보안 위협과 이에 대한 대응책을 중점적으로 다루었다. EV의 충전 과정 중 발생할 수 있는 다양한 보안 문제, 특히 차량 대 그리드 통신을 통한 에너지 도용 가능성과 이로 인한 프라이버시 침해 문제가 심도 있게 탐구되었다.

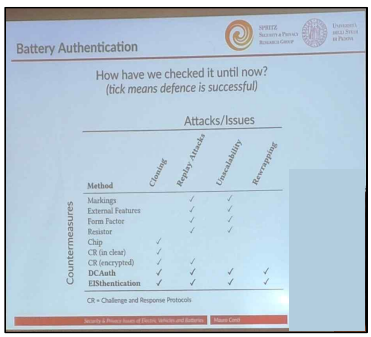
이 발표는 이전에 읽어 보았던 "Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)" 논문의 내용과 유사하게, EV 충전 프로세스의 보안 문제를 다루었다. 이 논문은 차량 충전 과정 중 데이터의 무단 접근이나 조작을 방지하는 다양한 기술적 대응책을 탐구하고 있다.

발표에서는 특히 EV 및 DWPT 기술이 가져올 수 있는 새로운 공격 표면에 대해 이야기했다. 예를 들어, 공격자가 차량 대 그리드 통신 표준을 이용해 에너지를 훔친 후 그 비용을 다른 사용자에게 전가하는 시나리오, 또는 충전 데이터를 통한 운전자 프로파일링 가능성 등이 이에 해당한다. 이러한 위협을 방지하는 방법으로는 물리적인 충전 정보의 보안 강화, 데이터 암호화, 사용자 인증 강화 등이 제안되었다.

특히, 강연자들은 양자 컴퓨팅 시대에도 견딜 수 있는 보다 안전한 자동차 통신 시스템 설계의 중요성을 강조했는데, 이를 통해 확실히 양자 컴퓨팅에 대한 우려와 관심이 높다는 것을 알 수 있었다.







Paper

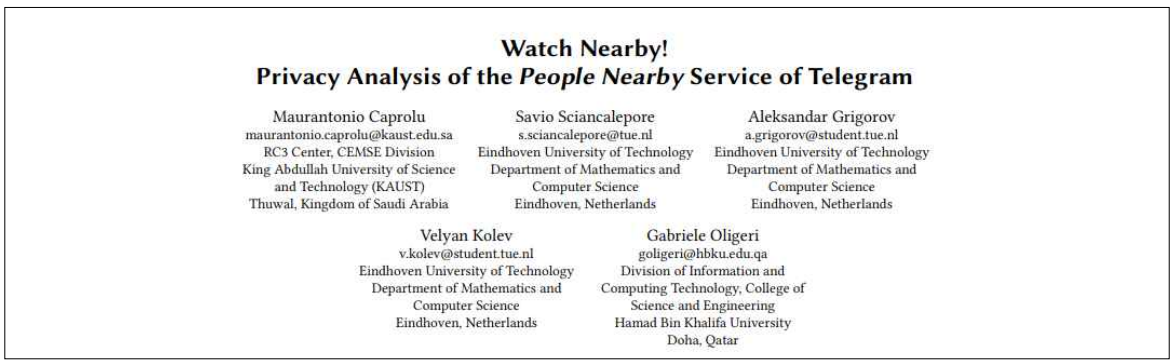
Watch Nearby! Privacy Analysis of the People Nearby Service of Telegram

Maurantonio Caprolu, Savio Sciancalepore et. al. (May 27)

이 논문은 텔레그램의 'People Nearby' 서비스가 제공하는 위치 프라이버시에 대해 체계적인 분석을 수행했다. 연구팀은 전 세계적으로 사용자의 위치를 조작하면서 텔레그램이 사용자 간의 거리를 어떻게 계산하는지 역공학적 방법으로 분석했다. 이를 통해 텔레그램이 주장하는 위치 프라이버시 반경 500미터가 실제로는 지리적 위치에 따라 달라지며, 극지방에 가까울수록 프라이버시 반경이 줄어들어 최소 128미터에 불과하다는 사실을 밝혀냈다.

이 연구는 텔레그램과 같은 인기 있는 통신 애플리케이션에서 위치 기반 서비스가 제공하는 프라이버시 보호가 얼마나 불충분한지를 드러내며, 사용자의 실제 위치 프라이버시가 텔레그램이 주장하는 것보다는 훨씬 낮다는 점을 시사한다. 이는 사용자들에게 잠재적인 프라이버시 위험을 초래할 수 있다.

연구는 체계적이고 광범위한 실제 측정을 통해 이루어졌으며, 이를 통해 'People Nearby' 기능의 위치 프라이버시의 실제 범위를 파악할 수 있다. 그러나 연구가 더 다양한 지리적 위치에서 시행되었다면 더 포괄적인 결과를 도출할 수 있었을 것 같다.



Watch Nearby!
Privacy Analysis of the *People Nearby* Service of Telegram

Maurantonio Caprolu
maurantonio.caprolu@kaust.edu.sa
RC3 Center, CEMSE Division
King Abdullah University of Science and Technology (KAUST)
Thuwal, Kingdom of Saudi Arabia

Savio Sciancalepore
s.sciancalepore@tue.nl
Eindhoven University of Technology
Department of Mathematics and Computer Science
Eindhoven, Netherlands

Aleksandar Grigorov
a.grigorov@student.tue.nl
Eindhoven University of Technology
Department of Mathematics and Computer Science
Eindhoven, Netherlands

Velyan Kolev
v.kolev@student.tue.nl
Eindhoven University of Technology
Department of Mathematics and Computer Science
Eindhoven, Netherlands

Gabriele Oligeri
goligeri@hbku.edu.qa
Division of Information and Computing Technology, College of Science and Engineering
Hamad Bin Khalifa University
Doha, Qatar

마치며

WiSec에서는 무선통신 분야뿐만 아니라 이동통신, 위성통신, 와이파이, UWB(초광대역) 통신 등 다양한 무선통신 기술들에 관한 연구뿐만 아니라 자동차, 배터리, 인공 지능, VR과 같은 다양한 플랫폼에서의 보안 문제 등을 포함한 30편의 논문이 발표되었다. 이러한 논문들은 다양한 관점에서의 첨단 보안 기술과 그 적용에 관한 연구 결과를 보여줘 보안 기술의 전방위적인 적용 가능성을 탐구하고 이해하는 데 큰 도움을 주었다.