MPC 기반 커스터디 시스템에서 패킷 손실에 따른 보안 임계점과 동적 보안 타임아웃 설계

최현명, 박민준, 김승민, 이흥노
광주과학기술원

viposition01@gm.gist.ac.kr, pmjun2005@gm.gist.ac.kr, seungminkim@gm.gist.ac.kr, heungno@gist.ac.kr

Security Thresholds and Dynamic Security Timeout Design under Network Packet Loss in MPC-based Custody Systems

Hyeonmyeong Choi, Minjun Park, Seungmin Kim, Heung-No Lee
Gwangju Institute of Science and Technology

요 약

본 논문에서는 MPC 기반 디지털 자산 커스터디 시스템에서 네트워크 패킷 손실이 보안 임계점에 미치는 영향을 분석한다. 다중 라운드 통신에 의존하는 MPC 서명에서는 미세한 패킷 손실이 서명 지연의 꼬리 지연(Tail Latency) 현상을 증폭시켜 고정된 타임아웃 정책 하에서 보안 취약점을 유발할 수 있다. 본 연구는 패킷 손실률을 공격자의 전략 변수로 모델링하고, 게임이론적 분석을 통해 시스템을 중단시키지 않으면서도 보안 예외(Fail-open)를 유도하는 최적의 공격 구간이 존재함을 보인다. 나아가 이러한 구조적 취약점으로 인한 보안 리스크를 억제하기 위해 네트워크 상태에 적응하는 동적 보안 타임아웃 메커니즘을 제안한다.

Ⅰ. 서 론

커스터디 시스템(Custody System)은 가상자산의 개인키를 제 3 자에게 위탁 관리하는 체계를 의미하며, 이 중 MPC(Multi-Party Computation) 기반 시스템은 개인키를 다수의 암호학적 조각으로 분산하여 단일 키 노출을 구조적으로 방지한다 [1],[2]. 그러나 MPC 구조는 다중 라운드 네트워크 통신을 전제로 하여 동작하며 [1], 이로 인해 MPC 기반 커스터디 시스템 보안 성능은 네트워크 상태에 직접적인 영향을 받는다. 특히 패킷 손실이나 지연과 같은 경미한 네트워크 열화는 서명 지연의 분포적 꼬리를 증폭시켜 [3], 고정된 보안 타임아웃 정책 하에서 예기치 않은 보안 공백을 초래할 수 있다. 공격자는 이를 악용해 시스템을 완전히 중단시키지 않으면서 서명 지연을 임계치 이상으로 유도할 수 있다. 이에 본 논문은 패킷 손실률과 보안 타임아웃 간의 상관관계를 정량적으로 모델링하고, 공격자의 기대 효용을 기반으로 게임이론적 분석을 통해 공격 유인이 형성되는 조건을 도출한다. 이를 바탕으로 고정 보안 타임아웃의 한계를 극복하기 위한 적응형 동적 보안 타임아웃 설계를 제안한다.

Ⅱ. 본 론

A. MPC 지연 모델 및 타임아웃 정책

MPC 서명 연산은 L개의 순차적인 네트워크 통신 라운드로 구성되며, 이는 단일 라운드의 지연이 전체 서명 완료 시간으로 누적 전파되는 구조적 특성을 갖는다. 패킷 손실률을 $p \in [0,1]$ 라 할 때, 각 라운드에서 지연을 유발하는 손실 이벤트가 발생할 확률 $L(p)$는 유효 패킷 수 S에 대해 $L(p) \triangleq 1-(1-p)^S$ 으로 정의된다.

이때 서명 완료 시간 $T(p)$는 기준 지연 시간 T_0와 i번째 라운드의 확률적 추가 지연 $X_i(p)$의 합으로 표현된다:

$$T(p) = T_0 + \sum_{i=1}^{L} X_{i(p)}\,. \tag{1}$$

여기서 $X_i(p)$ 는 패킷 손실 시 TCP 재전송 대기시간(RTO)으로 인해 발생하는 비선형적인 지연 특성을 반영한다. 본 연구는 평균 지연 시간보다 보안 정책의 트리거가 되는 지연 분포의 꼬리(Tail Latency)에 주목하며, 이를 정량화하기 위해 서명 연산이 보안 타임아웃 T_{sec} 를 초과할 확률 $\pi(p;T_{\mathrm{sec}})$을 다음과 같이 정의한다:

$$\pi(p;T_{\mathrm{sec}}) \triangleq Pr[T(p) > T_{\mathrm{sec}}]. \tag{2}$$

B. 타임아웃 처리 정책 모델과 Fail-open 의 정당성

금융 서비스의 가용성 확보를 위해 운영 주체는 타임아웃 발생 시 보안 검증을 완화하여 거래를 승인하는 정책적 예외, 즉 Fail-open 을 선택적으로 적용한다 [4]. 타임아웃 초과 시 거래 승인 사건 E_{open}의 조건부 발생 확률 $\phi(p;n)$은 다음과 같다:

$$\phi(p;n) \triangleq Pr\left(E_{open} \,\middle|\, T(p) > T_{sec},\ N = n\right). \tag{3}$$

여기서 N은 라운드 재시도 누적 횟수를 나타내는 상태 변수이다. 합리적 운영 정책 하에서 $\phi(p;n)$은 패킷 손실률 p가 과도하게 높거나 라운드 반복 횟수 N이 증가하여 공격 징후가 뚜렷해질수록 탐지 시스템에 의해 감소하는 경향을 가진다. 이러한 조건부 확률의 동적 특성은 공격

자가 무차별적인 네트워크 교란을 감행하는 대신, 시스템이 허용 가능한 범위 내에서 교묘하게 지연을 유발하도록 유인하는 핵심 요인으로 작동한다.

C. 보안 임계점과 공격자의 최적 전략 분석

본 연구는 공격자를 경제적 이득을 극대화하려는 합리적 주체로 정의한다. 공격자는 탐지 회피 범위 $p \in [0, p_{max}]$ 내에서 패킷 손실을 유도하며, 공격 성공 확률 P_{succ}는 다음과 같이 계산된다:

$$P_{succ} = \pi\,(p; T_{\mathrm{sec}}) \cdot \phi\,(p; n) \cdot \nu \cdot \tau. \tag{4}$$

이때 ν와 τ는 각각 자산 손실 및 트랜잭션 노출의 통계적 확률이다. 공격자 기대 효용 함수 U_A는 성공 시 이득 G와 공격 비용 $C(p)$를 고려해 다음과 같이 정의된다:

$$U_A = G \cdot P_{succ} - C(p). \tag{5}$$

p 증가 시 π는 상승하나 ϕ는 급감하고 비용 $C(p)$는 지수적으로 증가한다. 따라서 양 끝단($p \to 0$, $p \to p_{max}$)에서 U_A는 감소하며, 유효한 내부 구간 p^*에서 구조적인 극대점(Local Maximum)이 형성된다. 이는 공격자가 무차별 공격 대신, 보안 예외를 유도하는 '통제된 열화 전략'을 선택할 유인이 형성됨을 의미한다.

또한, 네트워크 지연은 E_{open}에 의한 위험뿐만 아니라 서명 라운드 재전송 횟수 증가에 따른 암호학적 부채널(Nonce) 누출 위험을 동반한다. 본 논문은 이를 라운드 진행 중 해킹 성공 확률 P_{move}로 정의한다. 본 연구에서는 해석적 분석을 위해 이산적인 재전송 이벤트를 연속 시간 t 에 대한 위험도 함수 $\lambda\,(t; p)$로 근사한다. 이러한 연속 근사는 이산적 재시도 모델에 대한 보수적 상계를 제공하므로, 실제 공격 성공 확률을 과소평가하지 않는다는 점에서 타당성을 갖는다. 단위 시간당 유효 이벤트 발생률 $r\,(t; p)$와 이벤트 당 치명도 $q\,(t; p)$는 다음과 같다:

$$r\,(p) = r_0 \frac{1 - p^R}{1 - p},\; q\,(t; p) = q_{min} + \frac{q_{max} - q_{min}}{1 + e^{-k(t-(m+np))}}. \tag{6}$$

여기서 R은 재전송 상한, $q(t; p)$는 시그모이드 형태의 치명도 증가 함수이다. $\lambda\,(t; p)$는 $r\,(t; p)$와 $q\,(t; p)$의 곱으로 정의된다. 이러한 모델 하에서 타임아웃 시점 T_{sec}까지의 누적 해킹 성공 확률 P_{move}는 다음과 같이 유도된다:

$$P_{move} = \left(1 - e^{\int_0^{T_{sec}} -\lambda\,(t;p)dt}\right) \cdot \tau. \tag{7}$$

D. 동적 보안 타임아웃 설계

본 절에서는 앞선 분석에서 도출된 구조적 취약점에 대응하기 위해, 관측된 네트워크 상태에 따라 보안 타임아웃을 조정하는 정책 설계를 제안한다.

고정된 T_{sec} 환경 하에선 공격자가 P_{succ}를 최대화하는 최적의 p^*를 학습하게 하는 구조적 취약점이 존재함을 보였다. 본 논문은 이를 해결하기 위해 관측된 패킷 손실률 $\hat{p}$에 따라 보안 타임아웃을 적응적으로 조정하는 함수 $T_{sec} = f(\hat{p})$을 제안한다. 두 위험 P_{succ}, P_{move}은 서로 다른 공격 표면이며, 본 논문은 보수적 설계를 위해 결합 확률의 상계로 합 h를 사용한다. 운영자는 정책 변수 T 를 조절하여 주어진 p에 대해 총 위험 h를 최소화한다:

$$h \triangleq P_{succ} + P_{move}. \tag{8}$$

총 위험 함수 h 의 임계점 조건 ($\frac{\partial h(p, T_{sec})}{\partial \mathrm{p}} = 0$) 을 이용하여 식 (4)와 식 (7)을 대입해 정리하면, 다음과 같이 적분 방정식 형태의 최적화 조건을 얻는다:

$$r\left(q_{max} T_{sec} + \frac{q_{max} - q_{min}}{k} \ln\left(\frac{1 + e^{-k(T_{sec} - (m+np))}}{1 + e^{k(m+np)}}\right)\right) = -ln(1 + \nu\pi\phi - C). \tag{9}$$

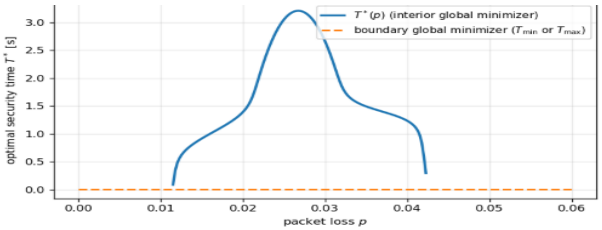

Fig 1. 임의 환경에서 p 에 따른 최적 동적 보안 타임아웃 T_{sec}

식 (9)를 만족하면서 h를 최소화하는 T_{sec} 곡선은 네트워크 열화 시 공격자의 기대 효용 상한을 제한하며, 구조적 최적점 형성을 방지한다. 이는 공격자가 특정 손실률을 목표로 하는 전략적 유인을 근본적으로 약화시킨다.

Ⅲ. 결론

본 논문에서는 MPC 기반 커스터디 시스템에서 네트워크 패킷 손실이 단순한 성능 저하가 아닌, 공격자의 전략적 변수로 악용될 수 있음을 분석하였다. 연구 결과, 고정된 보안 타임아웃 정책은 가용성 유지를 위한 Fail-open 위험 P_{succ}와 재전송에 따른 Nonce 누출 위험 P_{move} 사이에서 공격자에게 구조적 최적점 p^*을 제공하는 취약점이 있음을 도출하였다.

이에 대한 대응책으로 제안한 동적 보안 타임아웃은 관측된 네트워크 상태에 따라 총 위험 함수(h)를 최소화하는 최적의 임계점을 적응적으로 갱신한다. 이는 공격자의 기대 효용 상한을 수학적으로 제한하여, 네트워크 열화를 통한 전략적 공격 유인을 근본적으로 무력화하는 설계적 대안이 될 것이다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터지원사업의 연구결과로 수행되었음 (IITP-2026-RS-2021-II211835) 그리고 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. (RS-2025-22932973)

참 고 문 헌

[1] Y. Lindell and B. Pinkas, "Secure Multiparty Computation for Privacy-Preserving Data Mining," Journal of Privacy and Confidentiality, vol. 1, no. 1, pp. 59-98, 2009.

[2] Y. Lindell, A.Nof and S.Ranellucci, "Fast Secure Multi-Party ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody," Proc. ACM Conference on Computer and Communications Security (CCS), pp. 1837-1854, 2018.

[3] J. Dean and L. A. Barroso, "The Tail at Scale," Communications of the ACM, vol. 56, no. 2, pp. 74-80, Feb. 2013.

[4] J. Gray, "Why Do Computers Stop and What Can Be Done About It?" Proc. IEEE Symposium on Reliability in Distributed Software and Database Systems, 1986.