Hijacking Bitcoin:

Routing Attacks on Cryptocurrencies

✧ Summary

本篇旨在利用 Partition attack(分割攻擊)與 Delay attack(延遲攻擊)，而可一定程度地降低礦工的收益，且可令比特幣更易遭受 double spending、transaction filtering、selfish mining 等攻擊，甚至令商家、交易所交易受限，從而降低比特幣的易用性、價值，抑或造成貶值。

據作者所述，比特幣雖為分散式系統，然其高度的集中。不到 0.03%的 ISP 便託管了 30%比特幣節點，且 60%比特幣交易僅橫跨了 3 個 ISP。此外，網路為由多個 AS 所組成，並藉由 BGP 計算 forwarding path，而又比特幣訊息在傳遞時未進行加密且沒有完整性的保證。因此，attacker 能利用 internet routing infrastructure 的缺陷，透過 BGP hijacking 攔截比特幣流量；或是透過惡意的 ISP 在 forwarding path 上進行竊聽、修改、延遲、drop、inject 比特幣訊息、轉移比特幣流量。

✧ Strengths

Partition Attack 利用 BGP 未檢查 advertisement 正確性的特性，因此可藉由更明確的 prefix 來 hijack 節點的流量。最後便能透過這些假造資訊，致使其他 AS 會錯誤地導向流量，有效攔截在兩個 component 間的所有流量，切斷兩 component 所有連結，隔離兩邊區塊鍊的運算能力。作者透過 hijack prefixes 發現此攻擊在兩分鐘內便可攔截所有連線，而欲解決 hijacking 則需約數小時的時間。因而可達到某種程度上的 **DoS**；而對運算能力較差的一方，因為鍊較短者會被捨棄，也就造成**收益損失**；同時因所需等待確認的時間被延長，致使 **double spending** 更可能發生。

Delay Attack 利用如同 MitM 攻擊方式，能夠 drop 或修改 block message。因比特幣訊息的發送者或接收者不會檢查訊息是否被修改過，因此可令一些比特幣節點不會收到最新的 block 內容。對商家而言可能面臨**雙重支付問題**；對礦工而言可能白白**浪費了運算資源**；對節點而言可能**無法在 p2p 網路中互相合作**。

✧ Weaknesses

在 Partition Attack 方面，因為了控制足夠多的比特幣流量令攻擊生效，需控制足夠多 IP prefixes 才能進行全網路的 BGP hijacking。換言之，attacker 需發動具 AS 級別的攻擊，唯有到了 ISP 等級才能真的隔離兩 component 所有連結。此外，在實務上要攔截兩 component 間的所有流量實屬不易，只要有漏網之魚便會使分割攻擊失效，且因為攻擊範圍廣大，容易被察覺，使大家能及早防禦。再加上 multi-homing 的關係，某些節點間的訊息交換如同永久連結一般難以阻擋。

在 Delay Attack 方面，僅能針對**個人用戶**為目標，效果較有限，加上比特幣匿名性的緣故，使攻擊者不易鎖定目標。而延遲攻擊實際上也僅會讓部分節點收到訊息的速度減慢，仍不致於會瓦解整個加密貨幣體系。

此二攻擊基本上也都不難防範，有許多攻擊特徵可以**及早覺察**(如:延遲、斷線、異常 pattern)，而且**防禦方式也好部署**(如:端點加密、連結多樣性使路徑更隨機、調整 prefixes、MAC、使用多個 port)。

✧ Reflection

比特幣理論上為分散式系統、P2P network，但在實務運作上並沒有如大家所想像中的分散，也因為其匿名性而缺乏身分驗證與完整性檢查機制，才會使分割攻擊與延遲攻擊有效。有幸的是，此二攻擊實際上不大會瓦解比特幣運作機制，僅會對實務應用上造成不便、麻煩與延遲。

在防禦方面，儘管現在不存在能夠對付所有攻擊類型的解藥，但是部署的對策越多，比特幣用戶的防禦就會越有效。

比特幣的確提供許多優勢是一般貨幣無法給予的，然而比特幣也同時存在著法定貨幣所沒有的風險。因信任的基礎不同，或許沒有一種十全十美的貨幣，但我們可以依據應用需求，評估能承擔的不同類型風險，再行決定使用虛擬貨幣或法定貨幣。