POLOMĚR VÝBUCHU

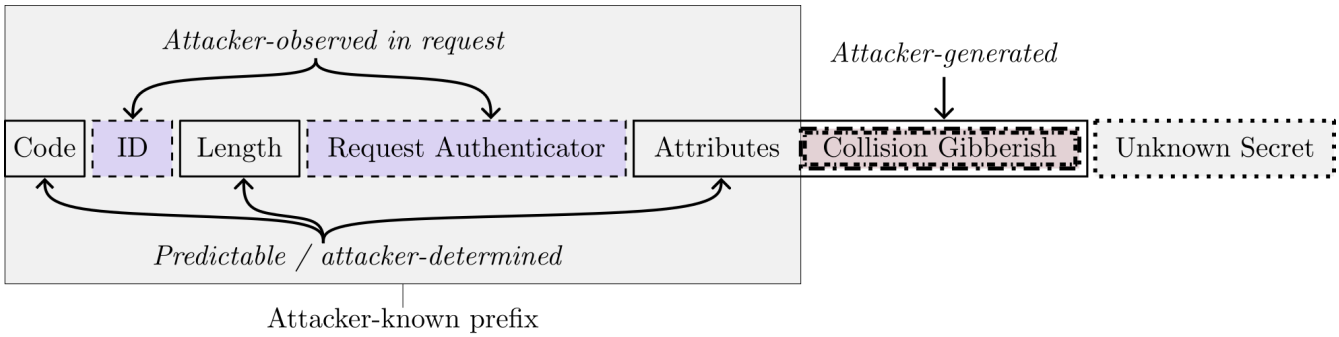

blastradius.fail/attack-details

Výbušný RADIUS útok podrobněji

Protokol RADIUS (Remote Authentication Dial-In User Service) je jádrem dnešní síťové infrastruktury. Ačkoli byl protokol poprvé navržen v roce 1991 — během éry vytáčeného internetu — zůstává de facto standardním lehkým ověřovacím protokolem používaným pro vzdálený přístup uživatelů a administrátorů k síťovým zařízením. RADIUS je podporován „v podstatě každým switchem, routerem, přístupovým bodem a VPN koncentrátorem prodaným za posledních dvacet let“ (zdroj).

V RADIUS se NAS (Network Access Server) chová jako klient, který ověřuje pověření koncového uživatele prostřednictvím požadavků RADIUS na centrální server. Klient a server RADIUS sdílejí pevné tajemství. Server odpoví zprávou o přijetí nebo odmítnutí (volané `Access-Accept`a `Access-Reject`). Požadavky a odpovědi mohou obsahovat označená pole nazývaná „atributy“, která specifikují různé parametry, jako je uživatelské jméno a heslo v požadavku nebo přístup k síti v odpovědi. Pakety požadavku obsahují hodnotu zvanou a, `Request Authenticator`která je v podstatě náhodná nonce. Pakety odpovědí obsahují hodnotu nazývanou `Response Authenticator`hodnota, která je určena k ochraně odpovědí serveru na integritu.

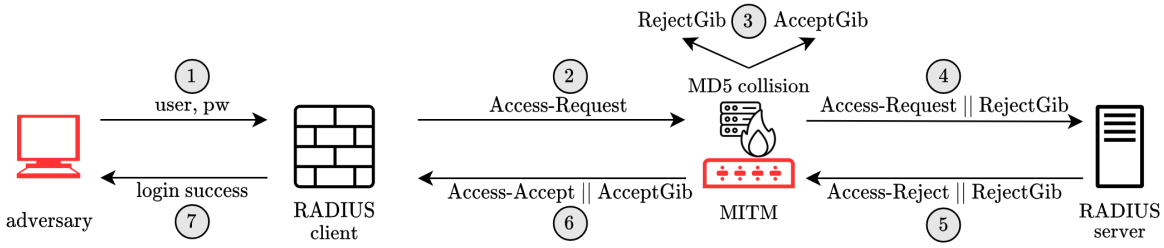
Vypočítá `Response Authenticator`se jako MD5(CÓdE||jáD||LEnGth||REquEst AuthEntiCAtÓr||PACkEt AttributEs||ShArEd SECrEt), MD5(CÓdE||jáD||LEnGth||REquEstAuthEntiCAtÓr||PACkEtAttributEs||ShArEdSECrEt), kde, jak ukazuje obrázek níže,jáDjáDaREquEst AuthEntiCAtÓrREquEstAuthEntiCAtÓrjsou náhodné hodnoty, které jsou v požadavku;CÓdECÓdE,LEnGthLEnGth, aPACkEt AttributEsPACkEtAttributEsjsou hodnoty v odpovědi serveru aShArEd SECrEtShArEdSECrEtje pevné sdílené tajemství, které klient a server znají, ale které útočník nezná.



V našem článku útočíme na tuto ad hoc `Response Authenticator`konstrukci RADIUS „MAC“. Náš útok umožňuje muži uprostřed mezi klientem RADIUS a serverem vytvořit platnou `Access-Accept`odpověď na neúspěšný požadavek na ověření. Útočník to provede vložením škodlivého `Proxy-State`atributu do platného požadavku klienta. Je zaručeno, že tento `Proxy-State`atribut bude serverem ve své odpovědi vrácen zpět. Útočník zkonstruuje `Proxy-State`tak, že `Response Authenticator`hodnoty mezi platnou odpovědí a odpovědí, kterou si útočník přeje zfalšovat, budou identické. Toto padělání způsobí, že NAS udělí protivníkovi přístup k síťovým zařízením a službám, aniž by protivník hádal nebo hrubě vynucoval hesla nebo sdílená tajemství.

Útok na kolize MD5, který využíváme, je verzí kolize se zvoleným prefixem od Stevense a kol. . Kolize zvolené předpony nám to umožňuje, pokud jsou dány odlišné předponyP1P1aP2P2k efektivnímu výpočtu nesmyslných blokůG1G1aG2G2takové, žeMD5(P1||G1)=MD5(P2||G2)MD5(P1||G1)=MD5(P2||G2). Když tak učiníme, struktura MD5 znamená, že pak můžeme připojit jakoukoli pevnou příponuSSa výsledné zprávy stále mají kolidující hodnoty hash MD5:MD5(P1||G1||S)=MD5(P2||G2||S)MD5(P1||G1||S)=MD5(P2||G2||S).

Stručně řečeno, následující obrázek ilustruje náš útok, když se RADIUS používá s PAP, protokolem pro ověřování hesla.



1. Protivník zadá uživatelské jméno privilegovaného uživatele a svévolně nesprávné heslo.

2. To způsobí, že klient RADIUS síťového zařízení oběti vygeneruje RADIUS `Access-Request`, který obsahuje 16bajtovou náhodnou hodnotu nazvanou `Request Authenticator`.
3. Protivník typu man-in-the-middle zachytí tento požadavek a použije `Access-Request`(včetně náhodného `Request Authenticator`) k předpovědi formátu odpovědi serveru (což bude, `Access-Reject`protože zadané heslo je nesprávné). Poté protivník vypočítá kolizi MD5 mezi předpovědí `Access-Reject`a `Access-Accept`odpovědí, kterou by chtěl vytvořit. Výsledkem jsou binární nesmyslné řetězce REjECtGibbErishREjECtGibbErishaACCEptGibbErishACCEptGibbErishtakové, že MD5(ACCEss-REjECt||REjECtGibbErish)MD5(ACCEss-REjECt||REjECtGibbErish) rovná seMD5(ACCEss-ACCEpt||ACCEptGibbErish)MD5(ACCEss-ACCEpt||ACCEptGibbErish).
4. Po vypočítání kolize muž-in-the-middle útočník přidáREjECtGibbErishREjECtGibbErishk `Access-Request`paketu, maskovaný jako `Proxy-State`atribut.
5. Server přijímající tuto změnu `Access-Request`zkontroluje uživatelské heslo, rozhodne se žádost odmítnout a odpoví paketem `Access-Reject`. Protože protokol RADIUS nařizuje, aby `Proxy-State`byly atributy zahrnuty do odpovědí,REjECtGibbErishREjECtGibbErishje připojeno k odpovědi. Kromě toho server vypočítá a odešle `Response Authenticator`, což je v podstatě MD5(ACCEss-REjECt||REjECtGibbErish||ShArEdSECrEt)MD5(ACCEss-REjECt||REjECtGibbErish||ShArEdSECrEt), za její `Access-Reject`reakci, aby se zabránilo neoprávněné manipulaci. Útočník nezná hodnotuShArEdSECrEtShArEdSECrEta nemůže předvídat nebo ověřit hash MD5.
6. Protivník zachytí tuto odpověď a zkontroluje, zda formát paketu odpovídá predikci ACCEss-REjECt||REjECtGibbErishACCEss-REjECt||REjECtGibbErish vzor. Pokud ano, protivník nahradí odpověď ACCEss-ACCEpt||ACCEptGibbErishACCEss-ACCEpt||ACCEptGibbErish a pošle jej s neupraveným `Response Authenticator`klientovi.
7. Kvůli kolizi MD5 se odesílatel `Access-Accept`odeslaný protivníkem ověřuje pomocí `Response Authenticator`, aniž by protivník znal sdílené tajemství. Klient RADIUS se tedy domnívá, že server schválil tento požadavek na přihlášení a udělil protivníkovi přístup.

Tento popis je zjednodušený. Zejména jsme museli provést kryptografickou práci, abychom rozdělili bláboly s kolizemi MD5 mezi více správně naformátovaných `Proxy-State`atributů a abychom optimalizovali a paralelizovali útok na kolize MD5 tak, aby běžel v řádu minut namísto hodin. Pro podrobný popis si prosím přečtěte náš dokument .