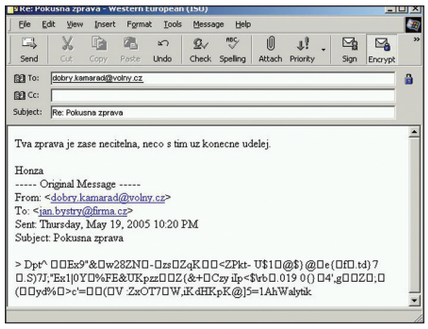
Kryptologie pro praxi – nebezpeční pavouci

Představte si, že vám od známého právě přišel elektronickou poštou šifrovaný dopis. Řekněme, že tento druh komunikace běžně používáte, takže na pozadí zápasu s právě uvařeným čajem a krabicí sušenek ležérně poklepáváte myší na ikonu šifrované zprávy, vkládáte čipovou kartu s privátním klíčem, zadáváte přístupový PIN, pokládáte šálek čaje, který vám intenzivně mlží brýle, uvažujete zda sušenky z předchozí krabice nebyly lepší, prostě rutina. Najednou však přichází zrada! V okně poštovního programu se místo textu zprávy objevili „pavouci“. Znáte je, potvory jedny – na první pohled se jedná o změť nejrůznějších znaků a symbolů připomínajících rozsypaný čaj a dost možná, že řadu z nich vidíte úplně poprvé. Není divu, že vašemu známému napíšete, aby si takové roztomilosti nechal pro sebe. Pro případ, že by snad nevěděl, o čem je řeč, tak mu v odpovědi rovnou ty nesympatické pavouky přibalíte. Právě jste vašemu známému odšifrovali a zaslali nějakou tajnou zprávu, ke které se původně neměl vůbec dostat!

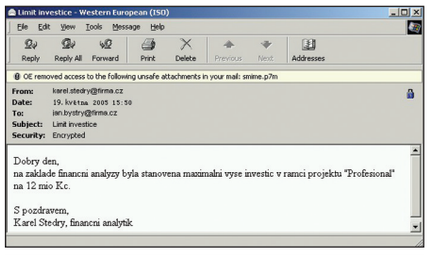
Matematická podstata

Metoda, kterou jsme si v úvodu představili, patří do kategorie útoků s voleným šifrovým textem. Útočník nejprve získá šifrový text, který chce vyluštit. V našem případě se jedná o zachycenou e-mailovou zprávu. Tento šifrový text určitým způsobem modifikuje a zašle jej napadenému kryptografickému modulu k odšifrování. Jemnější útoky nyní spoléhají na to, že podle chování modulu získají nějakou dílčí informaci, která jim při spojení s mnoha dalšími odezvami získanými pro jiné modifikace výchozího šifrového textu nakonec pomůže vyluštit celou zprávu (viz ST 3/2003 v [3]). Někdy však může jít analytik na věc doslova středem: pokud si kryptografické zařízení troufá rozlišovat otevřené texty podle toho, zda dávají či nedávají smysl, přičemž ty nesmyslné je ochotno komukoliv poskytnout, má útočník většinou předem vyhráno. V našem příkladu byl součástí kryptografického zařízení i nepříliš soustředěný uživatel, který naneštěstí právě rozhodoval o smysluplnosti odšifrované zprávy, a tak se stalo, že za záplavou pavouků netušil dovedně maskovaný text tajné zprávy.

Předpokládejme, že data luštěné zprávy byla zašifrována blokovou šifrou v modu CBC (ST 9/2003) a podívejme, se jak se dá takové „pavoučí“ maskování provést. Označme neznámé bloky otevřeného textu zprávy (včetně doplňku) $M=m_1, \ldots, m_N$. Víme, že pro bloky šifrového textu $C=c_0, c_1, \ldots, c_N$ platí $c_0=IV$, $c_i=E_k(m_i \oplus c_{i-1})$ pro $1 \le i \le N$. Označme $W=w_1, \ldots, w_N$ posloupnost maskovacích bloků, jejichž účelem bude po odšifrování na straně oběti zamlžit původní otevřený text zprávy. Konkrétní volba maskovacích bloků závisí jednak na předpokládaném obsahu zprávy, jednak na použitém poštovním programu, neboť ten musí být schopen maskovaný text zpracovat. Nicméně nejedná se o složitou úlohu, stačí jen trochu nanečisto experimentovat s příslušnou aplikací. S využitím C nyní sestavíme posloupnost bloků $Y=y_0, \ldots, y_{2N-1}$, kde $y_i=c_i/2 \oplus w_{i/2+1}$ pro $i=2k$ a $y_i=c_{(i+1)/2}$ pro $i=2k+1$, kde $0 \le k \le N-1$. Získanou posloupnost Y zabalíme do zprávy místo původního C a takto modifikovaný e-mail zašleme příslušné oběti. Ta po odšifrování obdrží otevřený text $X=x_1, \ldots, x_{2N-1}$, pro jehož bloky platí $x_i=D_k(y_i) \oplus y_{i-1}$, pro $1 \le i \le 2N-1$. Dosazením snadno ověříme, že pro bloky x_i, kde $i=2k+1$ pro $0 \le k \le N-1$, platí $x_i = D_k(c_{(i+1)/2}) \oplus c_{(i+1)/2-1} \oplus w_{(i+1)/2} = m_{(i+1)/2} \oplus c_{(i+1)/2-1} \oplus w_{(i+1)/2} = m_{(i+1)/2} \oplus w_{(i+1)/2}$. Vidíme, že liché bloky modifikovaného otevřeného textu obsahují lineárně maskované bloky původního otevřeného textu M. O sudé bloky X se příliš zajímat nemusíme, neboť pro nás zde nepředstavují příliš zajímavou informaci. Nyní stačí už jen vyčkat, až nám zmatená oběť zašle otevřený text X zpět s tím, že je pro ni nesmyslný. Pak s využitím posloupnosti W triviálně odmaskujeme příslušné bloky X, čímž získáme hledaný otevřený text M. Chtělo by se říct: „jak primitivní…“ a klasik by dále dodal: „… ale jak účinné!“



Obr. 1 Oběť odesílá útočníkovi cenná data v domnění, že se jedná o chybu.



Obr. 2 Útočník po odmaskování získává otevřený text luštěné zprávy.

Ostrý útok

Základní myšlenku maskování pro modus CBC popsanou výše je v praxi nutné ještě zasadit do kontextu konkrétního formátu použitého pro šifrované zprávy elektronické pošty. Zde se dnes nejčastěji setkáme se standardem S/MIME v.3 [2] v kombinaci s kryptografickými strukturami podle CMS [1]. Pro tuto kombinaci byl vytvořen i příklad zachycený na ilustračních obrázcích. Konkrétně se jednalo o hybridní šifrovací schéma, ve kterém byla vlastní zpráva šifrována symetrickou šifrou RC2 v modu CBC, jejíž náhodný klíč byl zašifrován asymetrickým algoritmem RSA. Z kryptologického hlediska je zde zásadní slabina v tom, že není použita bezpečná kontrola integrity šifrového či alespoň otevřeného textu. Útočník sice musí otevřený text maskovat tak, aby nepoškodil vnitřní hlavičky S/MIME (viz [2]), ale to lze jen stěží považovat za větší překážku. Rovněž vlastní formát zprávy podle CMS je z pohledu útočníka značně modulární a konfigurovatelný, a to prakticky bez kontroly integrity vyšší úrovně. Díky tomu je možné vytvářet ještě další, rafinovanější scénáře útoků než jen základní maskovací přístup předvedený v tomto článku.

Závěr

Ukázali jsme si typický útok moderní kryptoanalýzy, který dovedně využívá a kombinuje slabiny čistě kryptologické s chybami implementace, a v neposlední řadě také počítá s přičiněním lidského faktoru. Robustní protiopatření by se obdobně měla soustředit do všech tří směrů. V první řadě je velmi zarážející absence solidní kontroly integrity ve strukturách CMS tak, jak je běžně používá S/MIME a k němu příslušné aplikace.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] Housley, R.: Cryptographic Message Syntax (CMS) Algorithms, RFC 3370, August 2002

[2] Ramsdell, B., Ed.: S/MIME Version 3 Message Specification, RFC 2633, June 1999

[3] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz