Press Release

セキュリティフライデー株式会社
tel 0466-26-5666 / fax 0466-26-1130

2004 年 5 月 20 日　発表

社内の Windows ネットワークを監視し
弱いパスワードをハッカーより先に見つける監査技術を開発

セキュリティフライデー株式会社（藤沢市藤沢８９－１　社長：佐内大司）は、社内のファイルサーバへのログオンをネットワーク上で監視し、十分な強さを持たない脆弱なパスワードが利用されていた場合に、これをリアルタイムで検出する技術を開発いたしました。今後、この技術を利用して企業のセキュリティポリシに従って、パスワードを監査するシステムを開発していく予定です。

■概要

Windows を中心に構成されている企業内ネットワークにおいて、社員がファイルサーバへログオンする際、そのパスワードは暗号化されネットワーク上を流れるので、第3者に不正にネットワークパケットを取得されても、パスワードが直ちに漏洩してしまうことはありません。また、サーバに不正侵入されてしまった場合でも、パスワード情報は暗号化されて保存されている為、全てのパスワードがすぐに知られてしまうということはありません。このように Windows ファイルサーバへのアクセスパスワードは、暗号化により保護されており、推測されにくい十分な強さを持ったパスワードをユーザーが利用していれば、パスワードが短期間で漏洩してしまう心配はありません。（ただし、理論的には長い時間かければ解析が可能となります）

しかし、この暗号化パスワード方式においては、もしユーザーがすぐに推測されてしまうような弱いパスワードを使用してしまっている場合でも、管理者はそれを見つけることができず、結果として、弱いパスワードが使われ続けてしまう危険性が出てきます。情報漏洩対策やセキュリティ強化として、パスワードの正しい運用管理やパスワード監査は必要不可欠で、この暗号化されたパスワードの中から、ハッカーよりも先に弱いパスワードを見つけ出し、先手を打ってパスワードを変更させる必要があります。

今回開発した技術は、弱いパスワード（例：1ヶ月程度で暗号が解析されてしまうパスワード）のリストをコンピュータで演算処理した特殊なデータベースを大容量ハードディスクドライブに保有し、監査対象のネットワークから暗号化されたパスワードを取得、特殊データベースを利用して解析することで、弱いパスワードだけをリアルタイムに検出できるというものです。

■特長

- Windows ネットワークで利用される NTLM 方式のネットワーク認証に対応。
- 弱いパスワードだけを効率よく検出できる手法で、強いパスワードの解析には適さない。正しくパスワードが使われているサーバで悪用されることはなく、監査システムへの利用に最適。
- 弱いパスワードをリアルタイム検出するので、連続監査（常時監視）し弱いパスワードが使われると、ただちに（ハッカーより先に）これを検出可能。
- ネットワーク上を流れるパケットからの検出方式で、ネットワークやシステムへの変更が不要なシステムとして構築可能。

■仕様

- 解析時間およびデータベースサイズ（参考値）

解析時間		データベース・サイズ
従来（パスワード強度）	本方式	
32時間	2秒	0.25 Tbyte
7日	5秒	1.4 Tbyte
13日	9秒	2.5 Tbyte
30日	20秒	5.7 Tbyte

■今後の開発および販売計画

当社では、本技術を利用した企業内でのパスワード監査システムを、2004年秋を目標に製品化し、厳しいセキュリティ管理が要求されている官公庁や大手企業に対しての導入をはかります。

- 価格　　未定（個別見積もり）
- 受注生産

  ※悪用される可能性は低いシステムですが、悪用の可能性がゼロではないので、一般販売は行わず、信頼できるユーザーへの個別対応を予定しております。

■問い合わせ先

本件に関するお問い合わせは、

セキュリティフライデー株式会社（0466-26-5666, sales@securityfriday.com）　佐内／中岡まで

ウエブサイト　http://www.securityfriday.com/jp/