3A-1

モバイルネットワークにおける安全性評価情報提供サービス
Security Infomation Provider Service for Mobile Network

東 雄介 † 小畑 直裕 † 川口 信隆 †
Yusuke Azuma Naohiro Obata Nobutaka Kawaguchi
塩澤 秀和 ‡ 重野 寛 † 岡田 謙一 †
Hidekazu Shiozawa Hiroshi Shigeno Kennichi Okada

1. はじめに

近年, モバイル端末や無線 LAN の普及によりホットスポット等, モバイルネットワークサービスの増加・多様化が進んでいる. モバイルネットワークは外部から様々なユーザが接続するためネットワーク状況は動的に変化する. その一方, ネットワークの中には管理状態がずさんなものもあり, ユーザは満足の行くセキュリティ情報を得難い. そのため, ユーザは接続時にセキュリティ面で常に不安が残る.

そこで本稿では, ネットワークに接続している個人の端末から各ネットワークの状況の情報（IDS ログ）を収集・分析し, ユーザに動的な安全性評価情報を提供するセキュリティサービスを提案・実装し, モバイルネットワークでの安全かつ安心なネットワーク接続の実現を目指す.

2. 関連研究

ネットワークの様々な地点で IDS を設置し, 広範囲にわたってネットワークを監視することは, ネットワーク間での攻撃比較ができたり, 攻撃予兆の早期発見によって被害を抑制できるなど有益な点が多い. また,Stainford らは Cyber”Center for Disease Control” [1] という広域監視システムの有効性・必要性について言及している.

広範囲にわたるネットワークを監視するには複数の IDS をまとめて運用する必要があるが, 冗長なログが多量に出力され出現頻度の低いログを見落としがちになり, 新たな異常を見逃してしまうなどの問題がある.

竹森らが提案する IDS ログ分析支援システム [2] [3] では, 長期間のログ出力特性に対する短期間のログ出力特性の異常率, 他ネットワークのログ出力特性に対する注目ネットワークのログ出力特性の異常率を算出する. そして, その異常率を用いて検証不要な攻撃ログの示唆による冗長なログの排除, 効率的な異常ログの抽出を実現している.

しかし, 作業の省力化と分析の信頼性の向上を目的としたネットワーク運用者のためのシステムであり, ユーザに対する情報提供については考えられていない. ユーザには専門的知識のない者も多く, 分析結果のより簡易な形式での提示が必要となる.

3. 安全性評価情報提供サービス

ネットワークに接続している個人の端末から IDS ログを収集・分析し, ユーザに安全性評価情報を提供するサービスを提案する.

ユーザの要求としては,

- 複数ある接続先のネットワークの中で, どのネットワークが一番安全なのか
- ノート PC や PDA など自分のモバイル端末はそのネットワークにつないで大丈夫なのか, 安全に接続するために必要な対策は何か

などが, 主に考えられる.
そこで本サービスでは, 安全性評価情報として

1. **ネットワークの安全度ランキング** 算出した分析値の大小で出したランキング
2. **ユーザのホストの脆弱性マッチング** 脆弱性をつく攻撃の有無及びその対策法の提示

の 2 点を提供することで, ユーザの適切な対応を助け, 安全かつ安心なネットワーク接続を達成する.

3.1 サービスの手順

本サービスの手順を図 1 に示し, 以下に説明する.

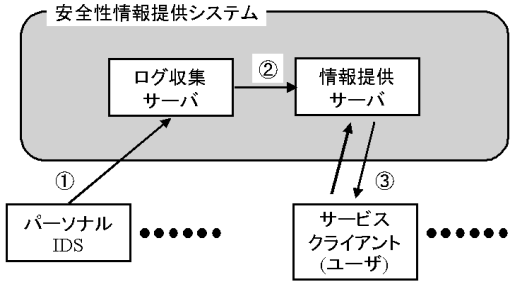

図 1: サービスの流れ

各構成要素は次のようになっている.

- **パーソナル IDS** 各ネットワークに接続している個人端末の IDS.IDS ログをログ収集サーバに定期的に送信
- **ログ収集サーバ** IDS クライアントから IDS ログを収集・抽出・分析し, 安全性評価情報を算出
- **情報提供サーバ** ログ収集サーバで算出した安全性評価情報を, サービスクライアントから受信したホストの脆弱性情報に対応させて提供
- **サービスクライアント（ユーザ）** 自ホストの脆弱性情報を送信, 安全性評価情報を取得

以下, サービスの流れを説明する.

1. ログ収集サーバがネットワークの様々な地点のパーソナル IDS(Snort [4] など) からのログを定期的に収集し, 必要な要素を抽出して分析, ネットワーク安全度ランキングを出す.

†慶應義塾大学理工学部
‡玉川大学工学部

2. 情報提供サーバは, ログ収集サーバで出した安全度ランキングをユーザのホストの脆弱性情報に対応させ, ユーザの脆弱性をつく攻撃の有無, その攻撃への対策法と共に提供する.
3. ユーザは, 取得した安全性評価情報から安全なネットワークに接続, もしくは安全となるようセキュリティレベルの変更を行う.

3.2 安全性評価情報

ここでは, 提供する安全性評価情報の詳細について説明する.

3.2.1 ネットワーク安全度ランキング

ネットワークによる比較, 時間による比較からネットワーク分析値, 時間分析値を算出し, その 2 つの分析値を元にした総合分析値を用いてランキングを出してユーザに提供する.

ネットワーク分析値とは, 他ネットワークのログ出力特性と比較した注目ネットワークのログ出力特性の異常を考慮した分析値であり, 時間分析値とは, 長期間のログ出力特性と比較した短期間のログ出力特性の異常を考慮した分析値である.

ネットワーク分析値

各攻撃イベント k につき, 注目ネットワーク m の情報提供端末数を N_{mk}, 検出数を E_{mk} とし,m を除いて n 個のネットワークがあるとき, 他ネットワーク l の情報提供端末数を N_{lk}, 検出数を E_{lk} として, ログ出力特性の異常を示す比率 r_k を,

$$r_k = \frac{E_{mk}}{N_{mk}} \Big/ \left\{ \sum_{l=1}^{n} \left(\frac{E_{lk}}{N_{lk}} \right) /n \right\} \tag{1}$$

で算出する. この比率を用いることで, 他ネットワークと比べた注目ネットワークの異常を注視することができる.

また各攻撃イベント毎に設定した危険度 d_k を用いて, 最近 x_j 分間での分析値 a_j を

$$a_j = \sum_{k} (E_{mk} \times d_k \times r_k) \tag{2}$$

で算出する.

そして最近 x_j 分の分析値を時間に応じてどの程度重要視するか定めた重み付けパラメータ p_j を用いてネットワーク分析値 W を

$$W = \sum_{j} (a_j \times p_j) \tag{3}$$

で算出する.

時間分析値

各攻撃イベント k につき, 最近 y_i 分の情報提供端末数を N_{yk}, 検出数を E_{yk}, 過去 z_i 分の情報提供端末数を N_{zk}, 検出数を E_{zk} として, ログ出力特性の異常を示す比率 r_{tk} を,

$$r_{tk} = \frac{E_{yk}}{N_{yk}} \Big/ \left(\frac{E_{zk}}{N_{zk}} \times \frac{y_i}{z_i} \right) \tag{4}$$

で算出する. この比率を用いることで, 注自ネットワークの過去に対する最近の異常を注視することができる.

また各攻撃イベント毎に設定した危険度 d_k を用いて, 過去 y_i 分間での分析値 a_{ti} を

$$a_{ti} = \sum_{k} (E_{yk} \times d_k \times r_{tk}) \tag{5}$$

で算出する.

そして最近 y_i 分の分析値を時間に応じてどの程度重要視するか定めた重み付けパラメータ p_{ti} を用いて時間分析値 T を

$$T = \sum_{i} (a_{ti} \times p_{ti}) \tag{6}$$

で算出する.

総合分析値

上記のネットワーク分析値 W, 時間分析値 T から総合分析値 A を,

$$A = W \times T \tag{7}$$

で算出し, この大小によりランキングを出す.

3.2.2 ユーザのホストの脆弱性マッチング

Windows のバージョンや Windows Update の履歴を示す xml ファイル (iuhist.xml) を用いてホストの脆弱性をチェックし, 各ネットワークでそのホストの脆弱性をつく攻撃の有無をマッチングする. そして, 該当ネットワークをピックアップし, 該当攻撃や脆弱性改善に必要なアップデートなど, 安全に接続するための対策を提示する.

上記の総合分析値を用いたランキングとユーザのホストの脆弱性マッチングの 2 点を安全性評価情報として提供する.

4. おわりに

本稿では, パーソナル IDS からの情報を用いた, モバイルネットワークでの安全性評価情報を提供するセキュリティサービスを提案した. 本サービスの利用により, ユーザの適切な対応を助け, 安全かつ安心なネットワーク接続を実現した.

参考文献

[1] Stuart Staniford,Vern Paxson,Nicholas Weaver: How to Own the Internet in Your Spare Time,Proceeding of the 11th USENIX Security Symposium (2002).

[2] 竹森 敬祐, 三宅 優, 中尾 康二, 菅谷 史昭, 笹瀬 巌: セキュリティデバイスログ分析支援システムの広域監視への適用, コンピュータセキュリティシンポジウム, pp. 397–402 (2003).

[3] 竹森 敬祐, 三宅 優, 中尾 康二: IDS ログ分析支援システムの提案, 情処技報, CSEC, 2003 年 5 月.

[4] Snort, http://www.snort.org/