# CONTAGION IN CYBERSECURITY ATTACKS

ADRIAN BALDWIN, IFFAT GHEYAS, CHRISTOS IOANNIDIS, DAVID PYM*, AND JULIAN WILLIAMS

ABSTRACT. We develop and estimate a vector equation system of threats to ten important IP services, using SANS-reported data over the period January 2003 to February 2011. Our results reveal strong evidence of contagion between such attacks, with attacks on ssh and Secure Web Server indicating increased attack activity on other ports. Security managers who ignore such contagious inter-relationships may underestimate the underlying risk to their systems' defence of security attributes, such as sensitivity and criticality, and thus delay appropriate information security investments.

## 1. INTRODUCTION

Information systems and their hosted applications are typically subject to information security flaws, which, if exploited, may lead to substantial losses for the organization. When such threats appear, security managers will deploy mitigating responses to secure their systems.

We characterize the operational status of systems in terms of their levels of sensitivity and criticality. Following well-established definitions (see, for example, [18] for a simple and elegant discussion), by sensitivity, we mean the level of security required for protecting data from access by unauthorized agents; by criticality, we mean the importance of the availability of accurate information for continuing system operations.

Security threats to data, its quality and accessibility, represent potential losses to the integrity of the operations of the organization. Security managers, in assessing the potential risks, should be interested in the relationship between the contagious threats to these different security attributes. The nature of the inter-relationship between the threats provides additional information to assist managers in making their choices of mitigating responses. For example, if the inter-relationship between threats is constant, independently of the frequency and intensity of threats, security managers can adopt smooth mitigation profiles to meet the threat. In the absence of such stable relationships, the managers' responses must be adjusted dynamically: for given temporal relationships between the number of attacks, their change (or 'jump') in frequency, and their change in size (extent of impact).

Theoretical aspects of contagion in information security have been addressed using game theory in [16, 14, 15, 7, 2]. These studies refer to the optimality of actions of both attackers and defenders and diverse system architectures. To our knowledge, there is no published empirical evidence regarding the statistical behaviour and inter-relationships between reported attacks on specific ports. Other, indirectly related work includes, for example, [4, 5, 6], where citations to other background work can also be found.

The aim of this paper is to develop a broad statistical framework to analyze the inter-relationship between the number of threats to (the ports — that is, process-specific software constructd serving as communications endpoints in a computer's operating system — for) critical services, such as email, databases, name and directory servers, website operations, and shared storage. We aim to assess the existence of contagious behaviour between these threats using threat data obtained by DShield and published by SANS (http://feeds.dshield.org).

In Section 2, we provide a basic causal model that relates the existence of threats to the sensitivity and criticality security attributes of a system, which focusses on the inter-relationship between the attributes and, subsequently, between the threats. In Section 3, we provide a characterization of the statistical methodology that is based upon the Hawkes process [8, 10, 9, 1], which is a model of contagion [1]. Section 4 discusses the data. The results and their implications for information security are presented in Section 5. Section 6 presents our conclusions concerning the nature of the relationships between the threats and the differential informational significance of some threats.

[*] Corresponding author: David Pym, University of Aberdeen, d.j.pym@abdn.ac.uk.

## 2. The Basic Model

We consider a security manager who must trade off criticality (C), sensitivity (S), and investment (K). Deviations of criticality $C_t$ and sensitivity $S_t$ (as functions of time, $t$) from their long-run targets $\bar{C}$ and $\bar{S}$, respectively, are linear functions of attacks on the various technological components of the system represented by the $m$-vector $X_t$. Therefore

$$\left\{C_t - \bar{C}, S_t - \bar{S}\right\} = \left\{w'_C X_t, w'_S X_t\right\} \tag{1}$$

where $w_C$ and $w_S$ are $m$ vectors of weights representing the vulnerability of the system to attacks (and $(\cdot)'$ denotes transpose). The relative values of these weights are determined, for a given instance of the model, by the relative intensities of attacks against the ports that are significant for these attributes. For the policy planner, the weights are assumed to be constant over a planning horizon $t, T$.

For the purposes of risk management, the security manager trades off total loss from criticality and sensitivity attacks against an costly investment profile, defined by the current level of investment $K_t$ and a long-run target $\bar{K}$, with the appropriate loss functions given by

$$\begin{aligned} L_{CS}\left(t,T\right) &= \int_t^T e^{-rt} f_C\left(C_t - \bar{C}\right) d\omega + \int_t^T e^{-rt} f_S\left(S_t - \bar{S}\right) d\omega \\ &\quad + \int_t^T e^{-rt} f_{CS}\left(C_t - \bar{C}, S_t - \bar{S}\right) d\omega \end{aligned} \tag{2}$$

$$L_K\left(t,T\right) = \int_t^T e^{-rt} f_K\left(K_t - \bar{K}\right) d\omega \tag{3}$$

where $r$ is a global discount factor, $\omega$ is the sample space of outcomes, and $f_C$, $f_S$ and $f_{CS}$ are affine functions that scale the measured deviations from target, $C_t - \bar{C}$ and $S_t - \bar{S}$, to a loss deriving from the deviation, $K_t - \bar{K}$, from the target profile of investment. The critical tipping point for additional investment occurs when $L_K\left(t,T\right) = L_{CS}\left(t,T\right)$. Similar models and conditions have been given in [11, 12, 13].

Assuming that $\bar{K}$, $w_C$, and $w_S$ are given, the security manager only has one vector stochastic integral to evaluate,

$$X\left(t,T\right) = \int_t^T g\left(X_\omega \mid \theta\right) d\omega \tag{4}$$

where $g(\cdot)$ characterizes a multivariate càdlàg (continue à droite, limite à gauche) process [3, 17] for the arrivals of attacks on the system, with vector of parameters $\theta$. Following [13], building on [12, 11], the system of equations can be uniquely characterized by the stochastic process driving threats:

$$L_{CS}(t,T) = f_C\left(w'_C X\left(t,T\right)\right) + f_S\left(w'_S X\left(t,T\right)\right) + f_{CS}\left(w'_C X\left(t,T\right) X'\left(t,T\right) w_S\right) \tag{5}$$

That is, a second-order Taylor expansion of the loss functions. Several important aspects emerge from this decomposition. If the threats are independent diffusions with homogenous moments and co-moments, then security investment may be approximated by a smooth investment profile. However, two further profiles may also exist: first, a set of independent, but self exciting, point processed will characterize a set of time homogenous discontinuities in this investment horizon; second, mutually self-exciting jumps in the attack process will characterize highly localized discontinuities in the investment profile.

## 3. The Statistical Methodology Based on the Hawkes Process

Vector processes that characterize attacks should allow for the following properties:

- Be represented as a vector stochastic differential equation (or, equivalently, stochastic integral equation) in order to support dynamic programming for forward-looking simulations and hence policy planning;
- Exhibit stochastic volatility in the diffusion process in order to capture potential changes in the variance of attacker behaviour and technological mechanisms of attacks;

- Exhibit discontinuous jumps that cluster in order to capture sudden changes in the vulnerability profile of systems/ports;
- Admit jumps that cluster across systems/ports, as attacks will most likely be multi-faceted (contagious).

The mathematical development in the remainder of this section establishes the necessary statistical methodology to support these features of our approach. The reader not wishing to follow the detailed mathematical development might proceed directly to Section 4.

We propose that the temporal evolution of the number of attacks incident upon a system can be characterized by the decomposition described below, based on a Brownian motion with stochastic volatility. In addition to the usual characterization in terms of a geometric Brownian motion, we allow for the existence of jumps — that is, discrete changes in volatility and size — in the specification. The usual geometric Brownian motion cannot accommodate such changes and does not admit contagion — that is, changes in the correlation between attacks based on characteristics such as size or frequency.

We therefore decompose the integral from Equation 4 into mutually self-exciting jump diffusion process, to capture potential contagion effects between attacks on different ports. Specifically, we adopt the Hawkes process [8, 10, 9, 1], a very general specification that captures the probability of jumps and allows for the parametric estimation of mutual self-exciting processes.

Equation 6 denotes the time evolution of an attack, given by the vector stochastic integral (4), which consists of a deterministic drift term ($u_i dt$), its own volatility term ($V_{i,t}$), and a jump term, $dN$ of size $Z$.

$$dX_{i,t} = u_i dt + \sqrt{V_{i,t}} dW_{i,t}^X + Z_{i,t} dN_{i,t} \tag{6}$$

where $dW_{i,t}^X$ is a Brownian motion. The volatility equation (7) is given a stationary stochastic process:

$$dV_{i,t} = k_i \left(\theta_i - V_{i,t}\right) dt + \eta_i \sqrt{V_{i,t}} dW_{i,t}^V \tag{7}$$

where $dW_{i,t}^V$ is a Brownian motion, $\theta_i$ denotes the long-term volatility, $k_i$ the speed of adjustment, and $\eta_i$ denotes the kurtosis.

The jump process $dN$ is assumed to be a Hawkes process, whose evolution can be expressed in terms of its intensity process $\lambda_{i,t}$,

$$\left\{ \begin{array}{l} \mathbb{P}\left[N_{i,t+\Delta} - N_{i,t} = 0 \left| F_t \right|\right] = 1 - \lambda_{i,t}\Delta + o\left(\Delta\right) \\ \mathbb{P}\left[N_{i,t+\Delta} - N_{i,t} = 1 \left| F_t \right|\right] = \lambda_{i,t}\Delta + o\left(\Delta\right) \\ \mathbb{P}\left[N_{i,t+\Delta} - N_{i,t} > 1 \left| F_t \right|\right] = o\left(\Delta\right) \end{array} \right. \tag{8}$$

where $N_{i,i+\Delta}$ is an $m$ point process counting the number of jumps in $(0, t+\Delta)$ for the $i = 1, \ldots, m$ processes in the system and $F_{i,t}$ is the conditional mean jump rate per unit of time. The jump intensities exhibit clustering according to the following dynamics:

$$\lambda_{i,t} = \lambda_{i,\infty} + \sum_{j=1}^{m} \int_{-\infty}^{t} g_{i,j}\left(t-s\right) dN_{j,s} \tag{9}$$

where $i = 1, \ldots, m$ and $s \leq t$, and $j = 1, \ldots, m$; the distribution of jumps $N_{j,s}$ is determined by that of the intensities $\lambda_{i,t}$, where $\lambda_{i,\infty}$ is the long-term intensity.

$$\lambda_i = \lambda_{i,\infty} + \sum_{j=1}^{m} \lambda_j \int_{-\infty}^{t} g_{i,j}\left(t-s\right) ds = \lambda_{i,\infty} + \sum_{j=1}^{m} \left( \int_0^{\infty} g_{i,j}\left(\omega\right) d\omega \right) \lambda_j \tag{10}$$

The vector function $g$ us assumed to follow an exponential decay of the form

$$g_{i,j}\left(t-s\right) = \beta_{i,j} e^{-\alpha_i (t-s)} \tag{11}$$

for coefficients $\beta_{i,j}$ giving expected instantaneous jump values and decay rates $\alpha_i$. In matrix form,

$$\Lambda = \Lambda_\infty + \Gamma \tag{12}$$

The overall association between the jumps of the different attacks is then captured by the matrix $G(\tau)$, where $\tau = t - s$:

$$G\left(\tau\right) = \left( \begin{array}{ccc} \beta_{11}e^{-\alpha_1 \tau} & \ldots & \beta_{1m}e^{-\alpha_1 \tau} \\ \vdots & \ddots & \vdots \\ \beta_{m1}e^{-\alpha_m \tau} & \ldots & \beta_{mm}^{-\alpha_m \tau} \end{array} \right) \tag{13}$$

The diagonal elements indicate the self-excitation of the process — that is, when a jump occurs, the likelihood of another jump increases — whereas the off-diagonal elements indicate the influence of jumps in other attacks on the evolution of its own jumps. The existence of non-zero off-diagonal elements is indicative of the need, as discussed in the introduction, for managers to adjust their security responses dynamically according to their observations of the total threat environment.

For the system of vector equations,

$$\begin{gathered} dX_t = udt + \sqrt{V_t}dW_t^X + Z_t dN_t \\ dV_t = \kappa\left(\theta - V_t\right)dt + \eta\sqrt{V_t}dW_t^V \\ d\lambda_t = \alpha\left(\lambda_\infty - \lambda_t\right)dt + \beta dN_t \end{gathered}$$

Sahalia et al. [1] identify the first three moment conditions as the expectations

$$\begin{aligned} &\mathbb{E}\left[\Delta X_t\right] = \left(\mu + \lambda M\left[1\right]\right)\Delta + o\left(\Delta^2\right) \\ &\mathbb{E}\left[\left(\Delta X_t - \mathbb{E}\left[\Delta X_t\right]\right)^2\right] = \left(\theta + \lambda M\left[2\right]\right)\Delta + \frac{\beta\lambda\left(2\alpha - \beta\right)}{2\left(\alpha - \beta\right)}M\left[1\right]^2\Delta^2 + o\Delta^2 \\ &\mathbb{E}\left[\left(\Delta X_t - \mathbb{E}\left[\Delta X_t\right]\right)^3\right] = \lambda M\left[3\right]\Delta \\ &+\frac{3}{2}\left(\eta\theta\rho^V + \frac{\left(2\alpha - \beta\right)\beta\lambda M\left[1\right]M\left[2\right]}{\left(\alpha - \beta\right)}\right)\Delta^2 + o\left(\Delta^2\right) \end{aligned} \tag{14}$$

where $\rho^V$ is the first-order autocorrelation coefficient of the intensities $\lambda_{i,t}$ and the $M[i]$ indicate the centred moments matrices, and the fourth moment (kurtosis) as

$$\mathbb{E}\left[\left(\Delta X_t - \mathbb{E}\left[\Delta X_t\right]\right)^4\right] = \lambda M\left[4\right]\Delta \left( \begin{array}{c} \frac{3\theta\eta^2}{2\kappa} + 3\theta^2 + 6\theta\lambda M\left[2\right] + \\ 3\lambda\left(\lambda + \frac{\left(2\alpha - \beta\right)\beta}{2\left(\alpha - \beta\right)}\right)M\left[2\right]^2 + \\ \frac{2\left(2\alpha - \beta\right)\beta\lambda M\left[1\right]M\left[3\right]}{\left(\alpha - \beta\right)} \end{array} \right)\Delta^2 + o\left(\Delta^2\right) \tag{15}$$

For more details of the estimation procedure via Generalized Method of Moments (GMM), see Sahalia et al. [1].

## 4. Data

Getting a reliable picture of the attack environment is very difficult. Most organizations are very sensitive about the details of a attacks and how they happen. Information is rarely shared. This makes it very hard to understand the attack environment and to speculate about how it will evolve as, for example, the use of cloud increases.

Organizations have many sources of information about attacks that may be incident upon their networks. One source of particular interest is firewall logs. Most, if not all, corporate networks will run a firewall that limits the traffic in and out of the corporate intranet according to some set of rules. Firewalls also log the network activity that they see, particularly the network traffic that is being dropped. Security teams examine firewall logs to get an indication of what attacks are occurring. The log files may show particular IP addresses that are running scans or particular network ports that are being attacked.

The dataset upon which this paper draws is taken from the output of the DShield community project (http://feeds.dshield.org).

- DShield is a community project — sponsored by SANS (http://www.sans.org) — that correlates firewall log files from many volunteer companies in order to paint a picture of the current treat environment.

- DShield consists in a client system that converts firewall log files (from many different vendors) into a standard format. These are then sent to a data collection engine where the data is aggregated and used to analyze attack trends.
- DShield has very wide global coverage and has become the dominant attack correlation engine. It has been used in the early detection of worms and is used to analyse attack patterns. Much of the work using DShield data has been done to analyze particular events rather than to understand the overall attack space.
- DSheild has been collecting data for close to a decade so in this paper we take a historical view of the data looking at its statistical properties rather than individual events.

For our statistical analysis, we picked ten particular services, sampled daily for the period 1 January 2003 to 28 February 2011. The services considered are given in Table 1 and the descriptive statistics are given in Table 2. Here we looked for ports that would typically be used to run services that we would expect to see offered as part of a cloud service (either to manage the service or to help build other services). We also included DNS as its correct functioning is fundamental to the internet. The ports considered are significant for different security attributes, such as sensitivity and criticality, to varying relative extents. For example, the Secure Web Server is highly significant for sensitivity and DNS is highly significant for criticality. A detailed analysis of these relative weightings is beyond out present scope and is not critical to the level of analysis presented here.

Since the primary purpose of this paper is to illustrate a model, we have not attempted to filter the DShield data for false positives. A paper with stronger empirical objectives would need to do so.

TABLE 1. Services considered in extracts of DShield attack data (http://feeds.dshield.org)

| Service | Port Number | Description |
|---|---|---|
| DNS | 53 | A service used to find the IP address of a particular service given its name |
| ssh | 22 | Secure shell. A program used to connect to computers remotely |
| Oracle | 80, 443 | A popular enterprise database used at the core of many business applications |
| SQL | 118 | Microsoft's database which is again used at the heart of many business applications |
| LDAP | 389 | A directory service that often contains the name and details of employees within a company and which is used to determine employees' rights to access business applications |
| Web Server | 80 | Used to run websites. There are many different applications that could be used here but popular ones are IIS and Apache |
| Secure Web Server | 443 | The secure part of a web server where traffic is encrypted using SSL. Usually used for highly sensitive transactions |
| Samba | 139, 455 | A shared drive used to store and share information within many organizations |
| Email (IMAP) | 143, 993 | The protocol used by many email clients to access an email server. Many web based email services also support this protocol |
| Email (SMTP) | 25, 465 | SMTP is used by some email clients to send an email to an email server, but it is also used to forward emails between different email servers as email is sent from the sender's email server to the recipients |

## 5. RESULTS AND ANALYSIS

Following the statistical methodology outlined in Section 3, we estimated have estimated the vector equation system given in Equations 14 and 15 by GMM. Inference was undertaken using the estimated

TABLE 2. Descriptive Statistics of the Attack Series

| | DNS | ssh | Oracle | SQL | LDAP |
|---|---|---|---|---|---|
| Mean | 331529 | 2782020 | 8334 | 929074 | 43042 |
| Standard Deviation | 307232 | 2964248 | 46118 | 867475 | 47517 |
| Skewness | 4 | 2 | 17 | 6 | 2 |
| Kurtosis | 33 | 11 | 345 | 67 | 7 |

| | Web Server | Secure Web Server | Samba | IMAP | SMTP |
|---|---|---|---|---|---|
| Mean | 787514 | 69568 | 200394 | 1426 | 20235 |
| Standard Deviation | 998963 | 83628 | 207624 | 4468 | 45661 |
| Skewness | 4 | 11 | 6 | 15 | 5 |
| Kurtosis | 22 | 250 | 72 | 329 | 36 |

information matrix of the system. Given the challenging dimensionality of the system, we are reporting a selection of our statistical results, which shed light on our choice of statistical model. Our model incorporates stochastic jumps to the geometric Brownian motion describing the evolution of attacks and also allows for the existence of mutually self-exciting processes. The parameters of interest are, therefore, represented by the estimates of $\lambda_\infty$ that are indicative of the existence of jumps. Contagion is captured by the elements of the contagion matrix (13).

All of the statistical results that are presented in the tables below are statistically significant at $5\%$.

Table 3 presents our estimates of $\lambda_\infty$ and the diagonal elements of the contagion matrix (13). Our estimated long-run intensities, $\lambda_\infty$, are modest and have similar values across all time series of attacks. Their statistical significance indicates that our choice of the inclusion of jumps in the law of motion of attacks is justified and that jumps constitute a significant, albeit unobserved, component of attacks.

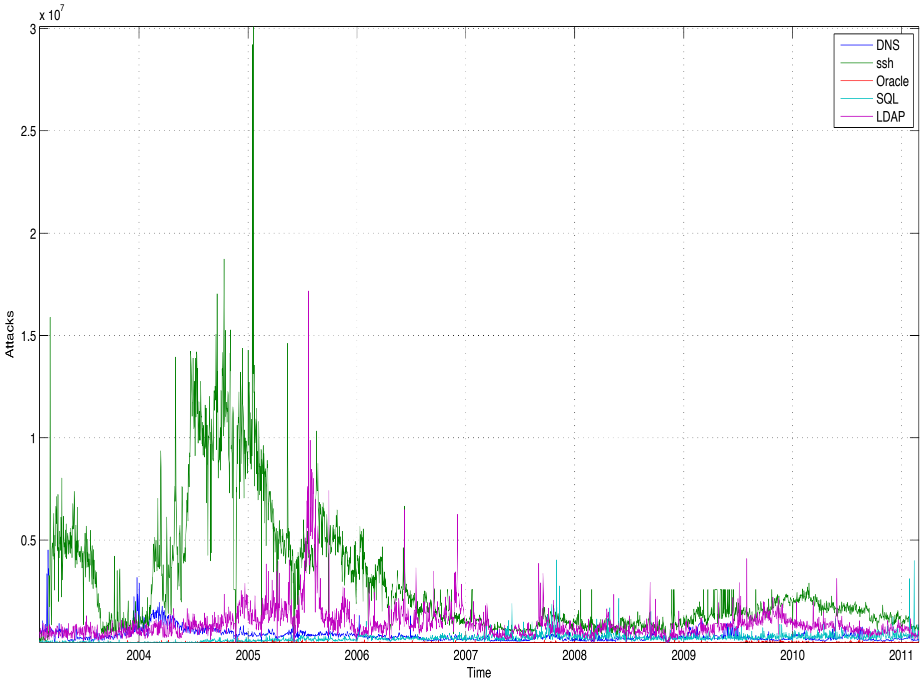

FIGURE 1. Attacks

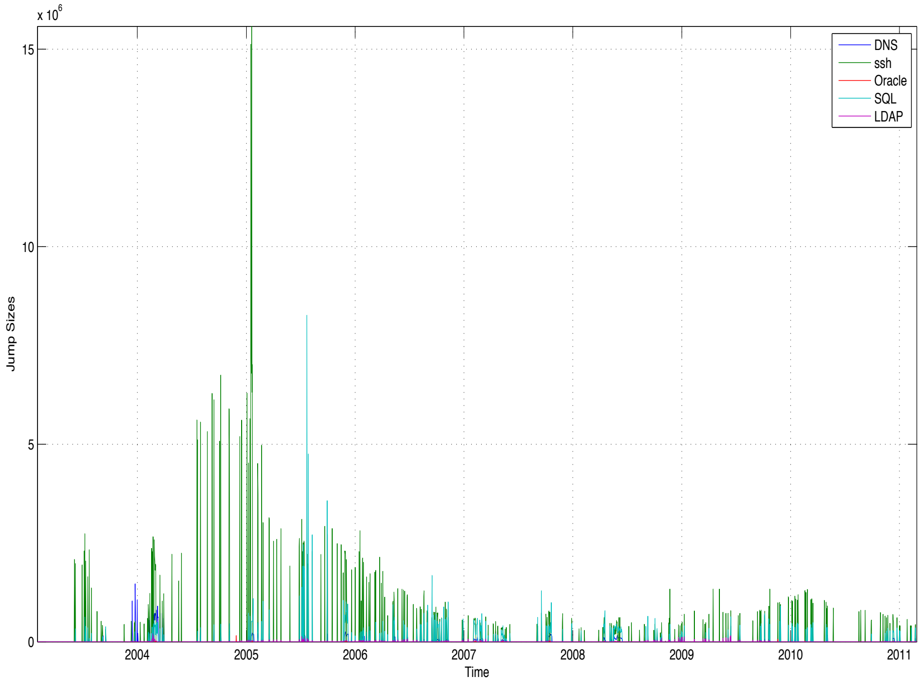

FIGURE 2. Jumps

Figures 1 and 2 (below) depict, respectively, the number of attacks and the estimated jumps for the first five listed services. The graphs for the second five would be similar. Informally, the graphs suggest that the correlation between the jumps will be stronger than can be inferred from the raw data.

The second row of Table 3 reports our estimates of the diagonal elements of the contagion matrix (13) and provides strong evident of the existence of self-exciting processes. It is remarkable that Secure Web Server exhibits the highest degree of self-excitation followed closely by ssh and IMAP.

Table 5 presents our estimates of the normalized elements of the correlation (contagion) matrix (13). By comparing these estimates with the corresponding values in the unconditional correlation (contagion) matrix given in Table 4, we establish the existence of uniformly high and positive correlations between attacks, so justifying our choice of the Hawkes process to capture evident of mutual self-excitement.

Once the jumps have been taken into account, the correlations between the intensity of attacks and their size are presented in Table 6. The structure of this matrix reveals that jumps cluster in both intensity and size, and that their associated is almost uniform and very strong. This correlation structure indicates that time evolution of the set of attacks will exhibit periods of intense activity and large size of attacks, and other periods where such activity is very low.

TABLE 3. Long-run Intensities; Diagonal Elements of $G$

| | DNS | ssh | Oracle | SQL | LDAP | Web Server | Secure Web Server | Samba | IMAP | SMTP |
|---|---|---|---|---|---|---|---|---|---|---|
| $\lambda_\infty$ | 0.1143 | 0.1158 | 0.1146 | 0.1114 | 0.1136 | 0.1118 | 0.1125 | 0.1132 | 0.115 | 0.1125 |
| $\beta_{i,j}e^{-\alpha_i\tau}$ | 0.0714 | 0.0831 | 0.17 | 0.05 | 0.0632 | 0.0728 | 0.1463 | 0.0443 | 0.0928 | 0.0085 |

We have computed the eigenvalues and corresponding eigenvectors of the contagion matrix (estimated in Table 5). The two highest eigenvalues (Table 7) associated with the filtered (i.e., to include jumps and mutual self-excitation) time series are $0.9894$ and $7.8643$. These represent approximately $90\%$ of all of the variation in the excitation process. This establishes the differential information content of attacks on

TABLE 4. Unconditional Correlation Matrix

| | DNS | ssh | Oracle | SQL | LDAP | Web Server | Secure Web Server | Samba | IMAP | SMTP |
|---|---|---|---|---|---|---|---|---|---|---|
| DNS | 1 | 0.46 | 0.02 | -0.37 | 0.21 | 0.44 | -0.01 | 0.09 | -0.10 | -0.26 |
| ssh | 0.46 | 1 | 0.18 | -0.14 | 0.50 | 0.42 | 0.03 | 0.12 | 0.12 | -0.26 |
| Oracle | 0.02 | 0.18 | 1 | 0.02 | 0.18 | 0.05 | 0.08 | 0.01 | 0.04 | 0.10 |
| SQL | -0.37 | -0.14 | 0.02 | 1 | 0.26 | -0.37 | 0.17 | 0.38 | 0.51 | 0.47 |
| LDAP | 0.21 | 0.50 | 0.18 | 0.26 | 1 | 0.18 | 0.11 | 0.32 | 0.35 | -0.06 |
| Web Server | 0.44 | 0.42 | 0.05 | -0.37 | 0.18 | 1 | 0.15 | -0.24 | -0.23 | -0.22 |
| Secure Web Server | -0.01 | 0.03 | 0.08 | 0.17 | 0.11 | 0.15 | 1 | -0.06 | -0.08 | 0.26 |
| Samba | 0.09 | 0.12 | 0.01 | 0.38 | 0.32 | -0.24 | -0.06 | 1.00 | 0.45 | 0.01 |
| IMAP | -0.10 | 0.12 | 0.04 | 0.51 | 0.35 | -0.23 | -0.08 | 0.45 | 1 | 0.04 |
| SMTP | -0.26 | -0.26 | 0.10 | 0.47 | -0.06 | -0.22 | 0.26 | 0.01 | 0.04 | 1 |

TABLE 5. Normalized $G$ Matrix

| | DNS | ssh | Oracle | SQL | LDAP | Web Server | Secure Web Server | Samba | IMAP | SMTP |
|---|---|---|---|---|---|---|---|---|---|---|
| DNS | 1 | 0.86 | 0.84 | 0.83 | 0.49 | 0.91 | 0.73 | 0.92 | 0.81 | 0.97 |
| ssh | 0.86 | 1 | 0.72 | 0.71 | 0.57 | 0.94 | 0.63 | 0.79 | 0.95 | 0.83 |
| Oracle | 0.84 | 0.72 | 1 | 0.99 | 0.41 | 0.76 | 0.88 | 0.91 | 0.68 | 0.86 |
| SQL | 0.83 | 0.71 | 0.99 | 1 | 0.41 | 0.75 | 0.89 | 0.89 | 0.67 | 0.85 |
| LDAP | 0.49 | 0.57 | 0.41 | 0.41 | 1 | 0.54 | 0.36 | 0.45 | 0.61 | 0.48 |
| Web Server | 0.91 | 0.94 | 0.76 | 0.75 | 0.54 | 1 | 0.67 | 0.84 | 0.89 | 0.88 |
| Secure Web Server | 0.73 | 0.63 | 0.88 | 0.89 | 0.36 | 0.67 | 1 | 0.79 | 0.59 | 0.75 |
| Samba | 0.92 | 0.79 | 0.91 | 0.89 | 0.45 | 0.84 | 0.79 | 1 | 0.75 | 0.95 |
| IMAP | 0.81 | 0.95 | 0.68 | 0.67 | 0.61 | 0.89 | 0.59 | 0.75 | 1 | 0.79 |
| SMTP | 0.97 | 0.83 | 0.86 | 0.85 | 0.48 | 0.88 | 0.75 | 0.95 | 0.79 | 1 |

TABLE 6. Correlation Between Services

| | DNS | ssh | Oracle | SQL | LDAP | Web Server | Secure Web Server | Samba | IMAP | SMTP |
|---|---|---|---|---|---|---|---|---|---|---|
| DNS | 1 | 0.86 | 0.86 | 0.89 | 0.88 | 0.81 | 0.84 | 0.87 | 0.89 | 0.87 |
| ssh | 0.86 | 1 | 0.86 | 0.86 | 0.83 | 0.83 | 0.84 | 0.84 | 0.87 | 0.87 |
| Oracle | 0.86 | 0.86 | 1 | 0.85 | 0.89 | 0.83 | 0.84 | 0.85 | 0.87 | 0.84 |
| SQL | 0.89 | 0.86 | 0.85 | 1 | 0.88 | 0.8 | 0.86 | 0.88 | 0.9 | 0.88 |
| LDAP | 0.88 | 0.83 | 0.89 | 0.88 | 1 | 0.86 | 0.83 | 0.87 | 0.9 | 0.83 |
| Web Server | 0.81 | 0.83 | 0.83 | 0.8 | 0.86 | 1 | 0.86 | 0.84 | 0.83 | 0.85 |
| Secure Web Server | 0.84 | 0.84 | 0.84 | 0.86 | 0.83 | 0.86 | 1 | 0.89 | 0.87 | 0.83 |
| Samba | 0.87 | 0.84 | 0.85 | 0.88 | 0.87 | 0.84 | 0.89 | 1 | 0.89 | 0.87 |
| IMAP | 0.89 | 0.87 | 0.87 | 0.9 | 0.9 | 0.83 | 0.87 | 0.89 | 1 | 0.86 |
| SMTP | 0.87 | 0.87 | 0.84 | 0.88 | 0.83 | 0.85 | 0.83 | 0.87 | 0.86 | 1 |

TABLE 7. Eigenvalues

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0.008 | 0.0219 | 0.0347 | 0.0582 | 0.084 | 0.1328 | 0.2664 | 0.5403 | 0.9894 | 7.8643 |

each port. From the corresponding eigenvectors, we infer that attacks on ssh and Secure Web Server are indicative of additional intensity and size of attacks on the remaining ports.

The totality of our statistical results supports our choice of filtering and reveals strong positive associations between attacks on the chosen ports, in contrast to the information suggested by the raw data that is indicative of weak associations, some of which have negative values. In the absence of our filtering, the use of the raw data might lead to erroneous responses by security managers in the face of attacks on specific ports. More specifically, the unconditional correlation between ssh attacks and IMAP is negative, but for the filtered series the corresponding correlation is positive and three times larger.

## 6. CONCLUSION

Our statistical analysis has revealed that attacks on individual ports are inter-related, with the relationships being exposed by the estimation of jumps and mutually self-exciting behaviour. From the ten chosen

TABLE 8. Eigenvectors for the Two Highest Eigenvalues

| DNS | ssh | Oracle | SQL | LDAP | Web Server | Secure Web Server | Samba | IMAP | SMTP |
|---|---|---|---|---|---|---|---|---|---|
| -0.0082 | -0.0919 | -0.4530 | 0.1689 | -0.5110 | -0.2563 | 0.3977 | 0.2114 | -0.3618 | 0.3118 |
| 0.1218 | 0.7169 | -0.0236 | 0.2244 | -0.2364 | 0.1687 | -0.4430 | 0.1447 | 0.0546 | 0.3403 |

services, attacks on ssh and the Secure Web Server account for almost all of the self-exciting behaviour. Failure to reveal such relationships may lead to erroneous investment profiles. For example, the unconditional correlation between ssh (the compromise of which brings high levels of threat to both criticality and sensitivity) and the Secure Web Server (typically used to support transactions requiring a high level of sensitivity protection) is approximately zero; but, after filtering, it is $63\%$ in the excited state. The responses of security managers should be based on this latter degree of correlation as it represents the impact of contagion on the level of risk that must be anticipated. For another example, introduced above, the unconditional correlation between ssh attacks and IMAP is negative, but for the filtered series the corresponding correlation is positive and three times larger.

The efforts of security managers to protect sensitivity and criticality at desired levels will necessitate additional costly investment at irregular intervals when faced with increased volume and diversity of attacks on, in particular, ssh and Secure Web Server. Such additional attacks will be associated with other additional attacks on all of the services considered.

An extension of the model would be to use the methodology in order to predict future levels of threat, so helping security managers to anticipate appropriate levels of investment. A refinement of the model would be to consider in more detail the mapping between the threats to services and the security attributes (such as sensitivity and criticality, or CIA) that may be compromised. Such an analysis might suggest how system architecture might be designed in order to limit the transmission of threats between services.

Other further work would be to consider how the behaviour of hackers correlates with our analysis of attacks. Such consideration is beyond the scope of this short paper.

## REFERENCES

[1] Yacine At-Sahalia, Julio Cacho-Diaz, and Roger J.A. Laeven. Modeling financial contagion using mutually exciting jump processes. Working Paper 15850, National Bureau of Economic Research, March 2010.

[2] Yoram Bachrach, Moez Draief, and Sanjeev Goyal. Security games with contagion. Manuscript, 2011: `http://www.econ.cam.ac.uk/faculty/goyal/wp11/securitygames17.pdf`.

[3] Patrick Billingsley. *Probability and Measure*. John Wiley & Sons, 1995.

[4] Rainer Böhme and Gaurav Kataria. Models and measures for correlation in cyber-insurance. In Ross Anderson, editor, *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006), Robinson College, University of Cambridge,* `http://weis2006.econinfosec.org`, 26–28 June, 2006. `http://weis2006.econinfosec.org/docs/16.pdf`.

[5] Rainer Böhme and Gaurav Kataria. A closer look at attack clustering. In Stuart Schecter, editor, *Proceedings of the I3P Workshop on the Economics of Securing the Information Infrastructure, Washington DC,* `http://wesii.econinfosec.org/workshop/`, October 23–24, 2006. `http://wesii.econinfosec.org/draft.php?paper_id=35`.

[6] Rainer Böhme and Galina Schwartz. Modeling cyber-insurance: Towards a unifying framework. In Tyler Moore, editor, *Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS 2010), Harvard,* `http://weis2010.econinfosec.org`, June 7–8, 2010. `http://weis2010.econinfosec.org/papers/session5/weis2010_boehme.pdf`.

[7] J. Grossklags, N. Christin, and J. Chuang. Security investment (failures) in five economic environments: A comparison of homogeneous and heterogeneous user agents. In *Proceedings (online) of the Seventh Workshop on the Economics of Information Security (WEIS)*, Hanover, NH, June 2008.

[8] A.G. Hawkes. Bunching in a semi-markov process. *J. Appl. Prob.*, 7:175–182, 1970.

[9] A.G. Hawkes. Point spectra of some mutually exciting point processes. *J. Roy. Statist. Soc.*, B 33:438–443, 1971.

[10] A.G. Hawkes. Spectra of some self-exciting and mutually exciting point processes. *Biometrika*, 58:83–90, 1971.

[11] C. Ioannidis, D. Pym, and J. Williams. Investments and trade-offs in the economics of information security. In Roger Dingledine and Philippe Golle, editors, *Proc. Financial Cryptography and Data Security '09*, volume 5628 of *LNCS*, pages 148–166. Springer, 2009. Preprint available at `http://www.abdn.ac.uk/~csc335/IoannidisPymWilliams-FC09.pdf`.

[12] C. Ioannidis, D. Pym, and J. Williams. Information security trade-offs and optimal patching policies. *European Journal of Operational Research*, 216(2):434–444, 2012.

[13] Christos Ioannidis, David Pym, and Julian Williams. Fixed costs, investment rigidities, and risk aversion in information security: A utility-theoretic approach. In *Proc. WEIS 2011, George Mason University, Fairfax, Virginia, 14-15 June, 2011*, 2011. Proceedings to be published by Springer (Bruce Schneier, editor) 2012. In press.

[14] M. Lelarge and J. Bolot. Network externalities and the the deployment of security features and protocols in the internet. In *SIGMETRICS*, 2008.

[15] Marc Lelarge. Economics of malware: Epidemic risks model, network externalities and incentives. In *Communication, Control, and Computing*, 2009.

[16] P. Parachuri, J. Pearce, M. Tambe, F. Ordonez, and S. Kraus. An efficient heuristic approach for security against multiple adversaries. In *AAMAS*, 2007.

[17] Philip Protter. *Stochastic Integration and Differential Equations 2nd Ed.* Springer, 2004.

[18] University of Georgia, Office of Information Security. Information Classification Standard. `http://infosec.uga.edu/policies/classification.php`, 2012.

HP LABS, BRISTOL
*E-mail address*: `adrian.baldwin@hp.com`

UNIVERSITY OF ABERDEEN
*E-mail address*: `igheyas@abdn.ac.uk`

UNIVERSITY OF BATH
*E-mail address*: `c.ioannidis@bath.ac.uk`

UNIVERSITY OF ABERDEEN
*E-mail address*: `d.j.pym@abdn.ac.uk`

UNIVERSITY OF ABERDEEN
*E-mail address*: `julian.williams@abdn.ac.uk`