Investments and Trade-offs in the Economics of Information Security

Presentation and Suggestions for Future Directions

Christos Ioannidis[1] David Pym[2] Julian Williams[3]

[1]School of Management, University of Bath

[2]Systems Security Lab,HP Labs, Bristol &
Department of Computer Science, University of Bath

[3]University of Aberdeen Business School, University of Aberdeen &
HP Labs

February 23, 2009

Outline of Talk

Motivation

- Information security and the network integrity are issues of the utmost importance to both users and managers.
- Such issues constitute growing concerns for policy makers, in addition to the legitimate concerns of the specialist technological community of experts.
- Our approach is to build a dynamic model of investment in information security.
- The model is based on the recognition that both IT managers and users appreciate the trade-off between the fundamental characteristics of information security, namely confidentiality and availability.

Prior Literature

- `Anderson et al (2007)`: Review of the cost of security breaches and fraud, issues in terms of technical and legal frameworks and offers recommendations.
- `Gordon and Loeb (2002)`: The economics of information security within the context of an optimizing framework.
- `Hausken (2006)`: Investment and information security and vulnerability.
- `Willemson (2007)`: existence levels of expenditure, a quantized approach to investment.

Our Approach

Utilise the library of tools available in the Economic and Finance Literature, to assist in the decision making process regarding information security.

- We can use Utility theory and Welfare Maximisation to create comparable measures.
- Use our convexity measures and concave utility functions to build weighting functions to assist in the optimal control problem.
- Model this in a dynamic framework with realistic control instruments.

General Linear Stabilisation Model

Following Giannoni and Woodford (2002), the general discrete time linear stabilisation policy problem can be expressed as a solution to the following control problem,

$$G \begin{bmatrix} Z_{t+1} \\ E_t z_{t+1} \end{bmatrix} = A_1 \begin{bmatrix} Z_t \\ z_t \end{bmatrix} + A_2 r_t + A_3 u_t \tag{1}$$

Loss Functions

The objective of the policy is to minimise the quadratic objective function in terms of squared deviations of the variables of interest Π from some a-priori specified target values Π^* by choosing the appropriate value of r given the structure of the system, the loss function,

$$\Lambda = E_t \left\{ \sum_{t=0}^{T} \frac{\delta^{-t}}{2} \left(\Pi - \Pi^*\right)^{\mathsf{T}} \Omega \left(\Pi - \Pi^*\right) \right\} \tag{2}$$

enshrines the policy makers basic preferences.

Essential Approaches

To use this model framework, we need two basic things:

- A system model describing the dynamic evolution of the variables in question.
- A set of utility functions outlining the preferences of the policy maker/administrator relative to that system.

Essential Approaches

To use this model framework, we need two basic things:

- A system model describing the dynamic evolution of the variables in question.
- A set of utility functions outlining the preferences of the policy maker/administrator relative to that system.

Essential Approaches

To use this model framework, we need two basic things:

- A system model describing the dynamic evolution of the variables in question.
- A set of utility functions outlining the preferences of the policy maker/administrator relative to that system.

CIA, Investments, and Trade-offs

- Organisations deploy systems technologies in order to achieve their business objectives.
- Organisations invest in deploying information security policies, processes, and technologies in order to protect three identified areas of concern:
  - the confidentiality, C,
  - integrity, I,
  - and availability, A, processes.

CIA, Investments, and Trade-offs

- Organisations deploy systems technologies in order to achieve their business objectives.
- Organisations invest in deploying information security policies, processes, and technologies in order to protect three identified areas of concern:
  - the confidentiality, C,
  - integrity, I,
  - and availability, A, processes.

CIA, Investments, and Trade-offs

- Organisations deploy systems technologies in order to achieve their business objectives.
- Organisations invest in deploying information security policies, processes, and technologies in order to protect three identified areas of concern:
  - the confidentiality, C,
  - integrity, I,
  - and availability, A, processes.

CIA, Investments, and Trade-offs

- Organisations deploy systems technologies in order to achieve their business objectives.
- Organisations invest in deploying information security policies, processes, and technologies in order to protect three identified areas of concern:
  - the confidentiality, C,
  - integrity, I,
  - and availability, A, processes.

CIA, Investments, and Trade-offs

- Organisations deploy systems technologies in order to achieve their business objectives.
- Organisations invest in deploying information security policies, processes, and technologies in order to protect three identified areas of concern:
  - the confidentiality, C,
  - integrity, I,
  - and availability, A, processes.

CIA, Investments, and Trade-offs

- Organisations deploy systems technologies in order to achieve their business objectives.
- Organisations invest in deploying information security policies, processes, and technologies in order to protect three identified areas of concern:
  - the confidentiality, C,
  - integrity, I,
  - and availability, A, processes.

Setting up the CIA Stabilization Model

- We postulate a system whose optimal operational state $(\bar{C}, \bar{A})$ is below its maximal capacity.
- In our initial case, The control mechanism in both cases is

$$R = \frac{1}{1-\xi}, \text{for } \xi \in [0, 1) \tag{3}$$

- which may be thought of as capturing the complexity of the system via the extent to which the system is `inter-connected`.

System Equations

The time evolution of confidentiality and availability are described in Equations 4 and 5. C_0 is an initial value.

$$C = -\alpha(P)\left(\int_{t_0}^{t}\dot{A}\,dt\,\left(\beta\int_{t_0}^{t'}\dot{K}\,dt'\right)^{-1}\right)+C_0 \quad (4)$$

$$A = \gamma\left(\int_{t_0}^{t'}\dot{R}\,dt'\right)+\delta\left(\int_{t_0}^{t'}\dot{K}\,dt'\right)-\epsilon\left(\int_{t_0}^{t'}\dot{C}\,dt'\right) \quad (5)$$

where $t' < t$.

System Equations II

Investment in information security is triggered by fluctuations in availability and the time dynamics of this are expressed in Equation 6

$$\dot{K} = -\eta \dot{A} \tag{6}$$

The system responds to deviations in confidentiality, as given by Equation 7:

$$\dot{R} = x\left(C - \bar{C}\right) \tag{7}$$

Note that as $t' \rightarrow \infty$, the system stabilises.

Utility Maximisation Problem

- The decision makers optimal control problem is as follows:

$$L(C, A, \dot{K}) \quad = \quad E\left(w_1(C - \bar{C})^2 + w_2(A - \bar{A})^2 + w_3(\dot{K} - \bar{\dot{K}})^2\right)$$

- The loss function, whose solution will be of the form

$$L\left(R\right) \quad \triangleq \quad \min_x L(C, A, \dot{K}) \tag{8}$$

- Where x is a control variable.
- In this case, the optimal control issue is based on convex preferences relative to a given set of targets, $\bar{C}$, $\bar{A}$ and $\bar{\dot{K}}$.

Stability Conditions

Using a simple Euler Scheme, the system is discretized, the stability condition from this scheme is as follows,

$$\begin{aligned}\varsigma = \; & Z^5 - Z^4 + \left(-\ln(\epsilon)\ln(\alpha) + \ln(\delta)\ln(\eta)\right) Z^3 + \\ & + \left(\ln(\epsilon)\ln(\alpha) - \ln(\theta)\ln(\alpha)\ln(\gamma) + \ln(\epsilon)\ln(\beta)\ln(\eta)\right) Z^2 + \\ & + \left(\ln(\theta)\ln(\beta)\ln(\gamma)\ln(\eta) - \ln(\delta)\ln(\eta)\right) Z \\ & + \ln(\theta)\ln(\beta)\ln(\gamma)\ln(\eta) - \ln(\epsilon)\ln(\beta)\ln(\eta)\end{aligned}$$

Parameter Arrangements and Impulse Responses

- To elucidate the impact of a single non-persistent shock to confidentiality, C_t, the impulse response of C_t to a shock to P_t at $t = 0$ is derived numerically.
- For tractability and exposition, the system responses are illustrated as a percentage deviation from equilibrium of the system following a single unit-shock to confidentiality (i.e., we assume that $P_{t=0} = 1$).

Example 1: C versus A

- We compare the behaviour of Organization 1, such as a deep-state or intelligence agency, which weighs confidentiality more highly than availability, with Organization 2, such as an online retailer, which weighs availability more highly than confidentiality.
- These preferences are expressed by the relative values of w_{11} and w_{12}. We assume, for simplicity, that the organizations are similar in all respects.

Example 1: C versus A

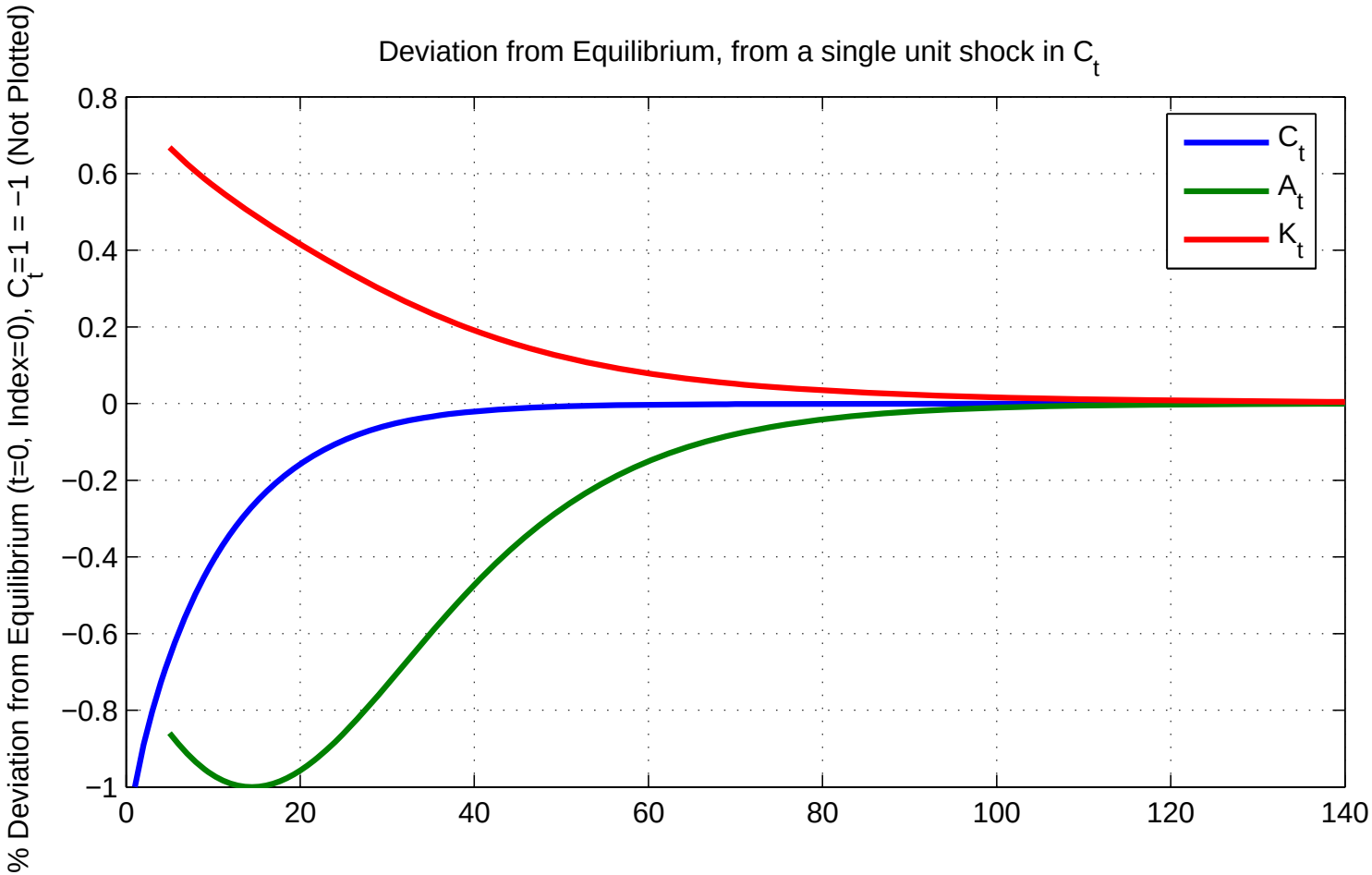


Figure: Confidentiality (w_1) versus Availability (w_2), Response of System

Example 1: C versus A

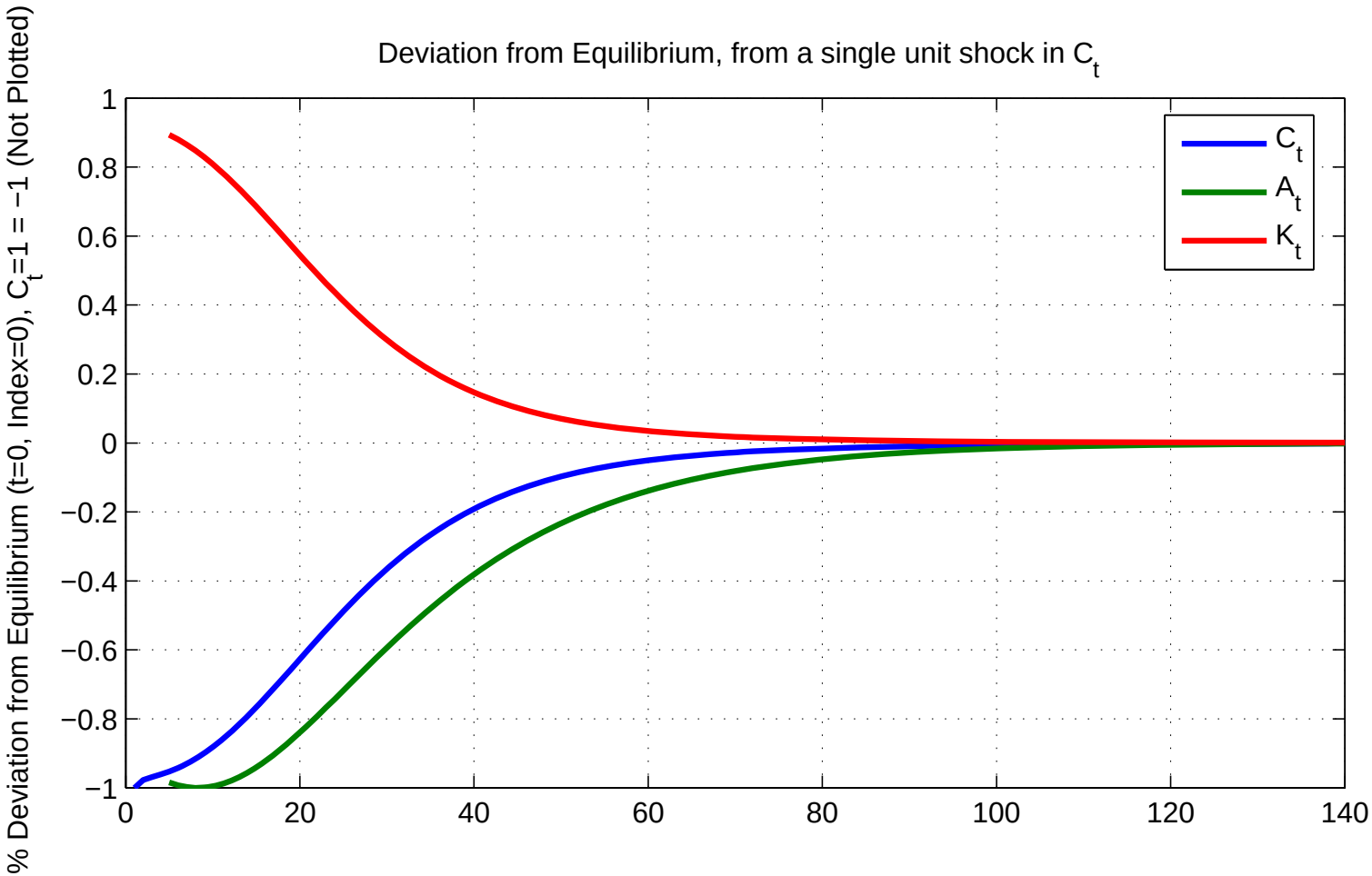


Figure: Confidentiality (w_1) versus Availability (w_2), Response of System

Example 1: C versus A

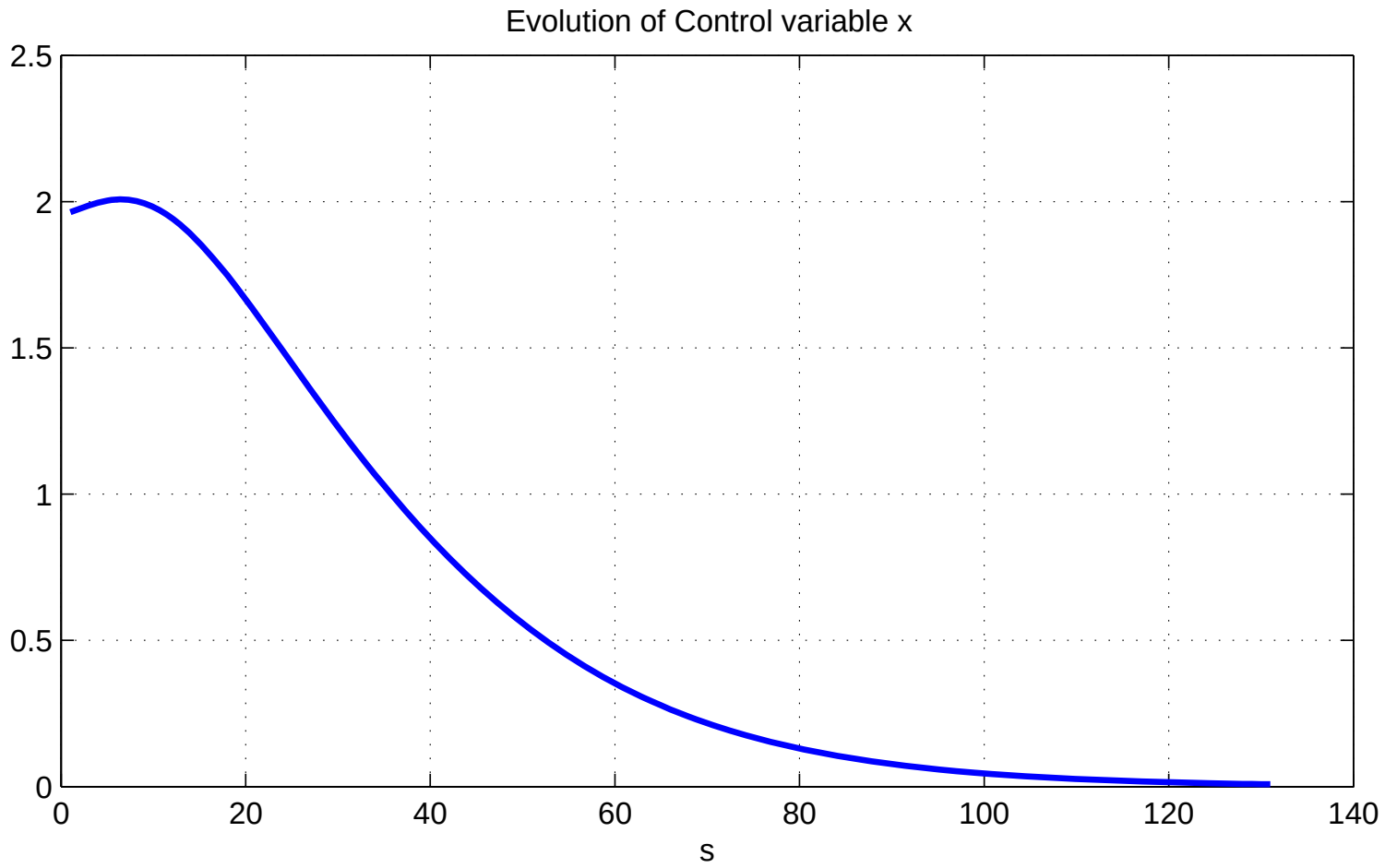


Figure: Confidentiality (w_1) versus Availability (w_2), Response in Instrument

Example 1: C versus A

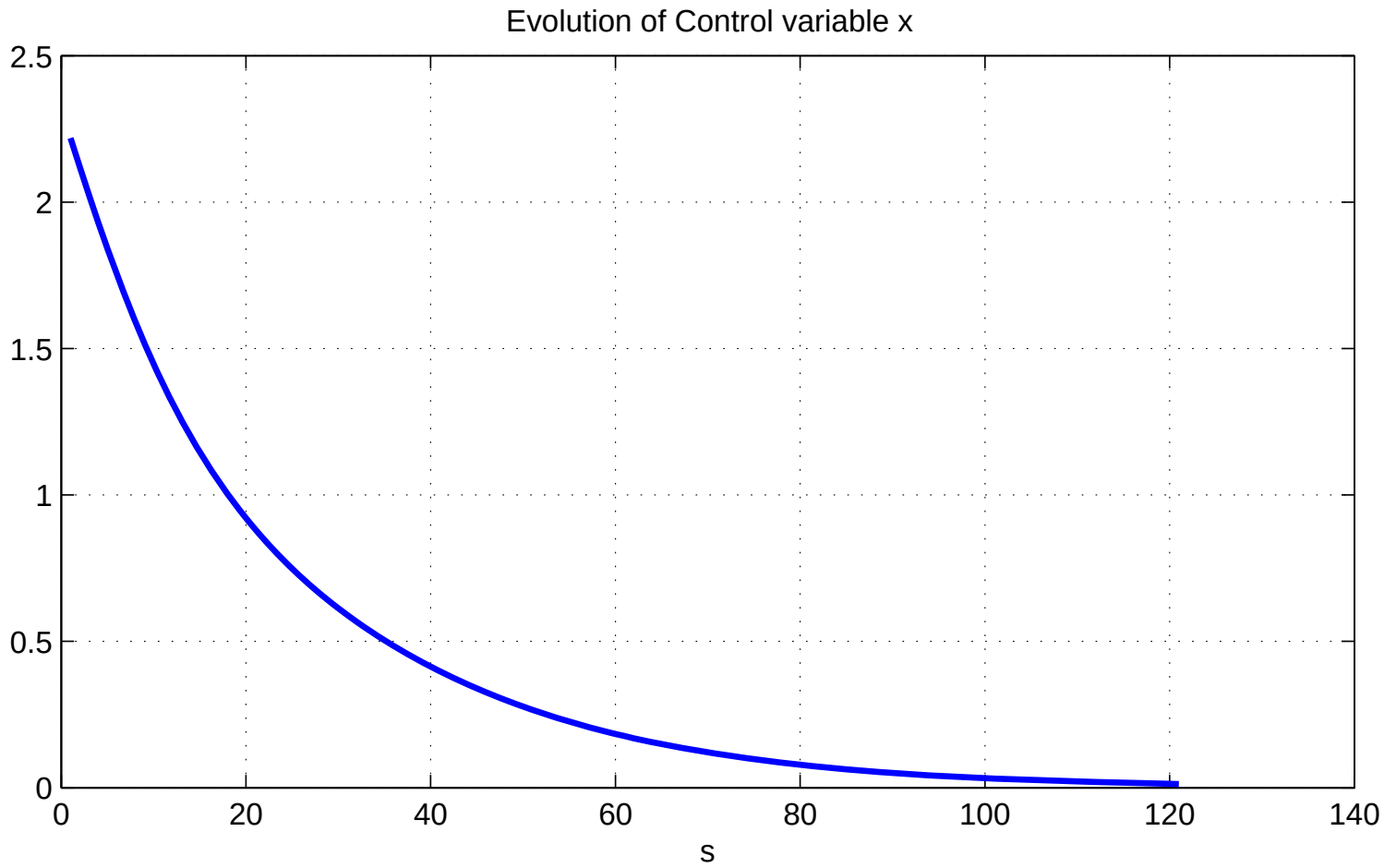
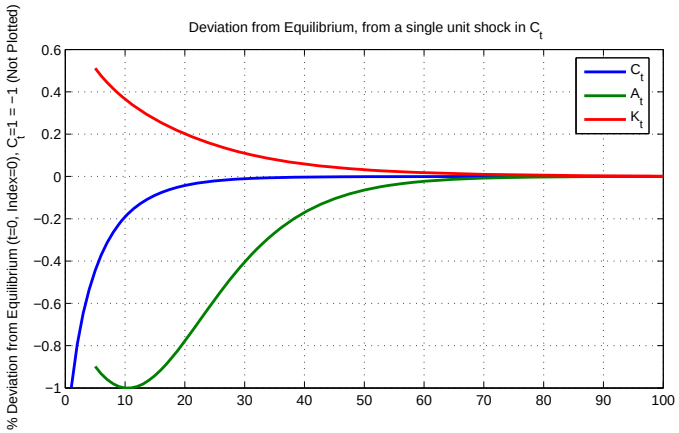


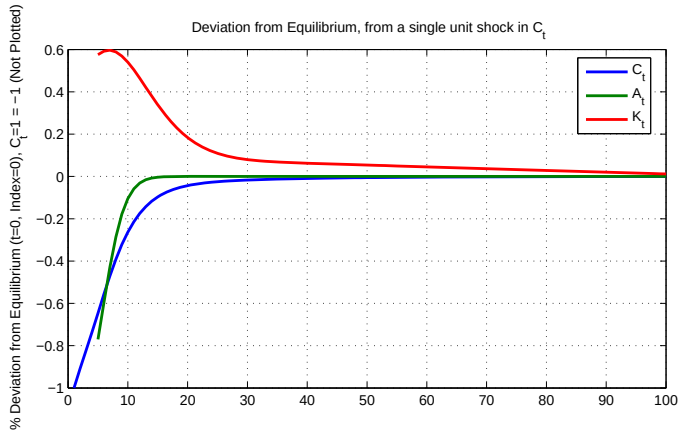
Figure: Confidentiality (w_1) versus Availability (w_2), Response in Instrument

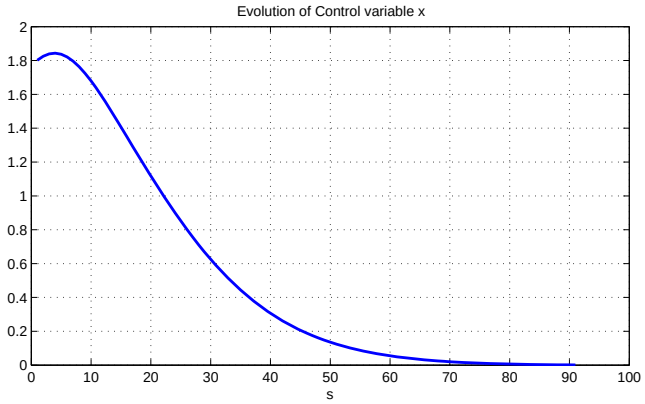
Example 1: C versus A

- The recovery of confidentiality and availability to their pre-shock levels is consistent with the managers' preferences. Measures are taken to restore the system's degree of confidentiality rapidly by enforcing prolonged periods of reduced inter-connectedness.
- In Organization 1, capital in information security increases almost immediately and then declines monotonically whilst for Orgainzation 2, both confidentiality and availability are restored at almost the same rate whilst capital in information security is of relatively smaller size and it achieves it maximum few periods after shock, exhibiting a somewhat slower rate of return to 'equilibrium'.

Example 2: A as Priority







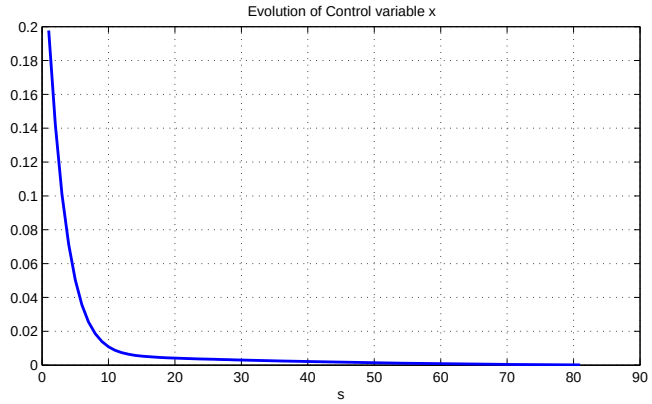
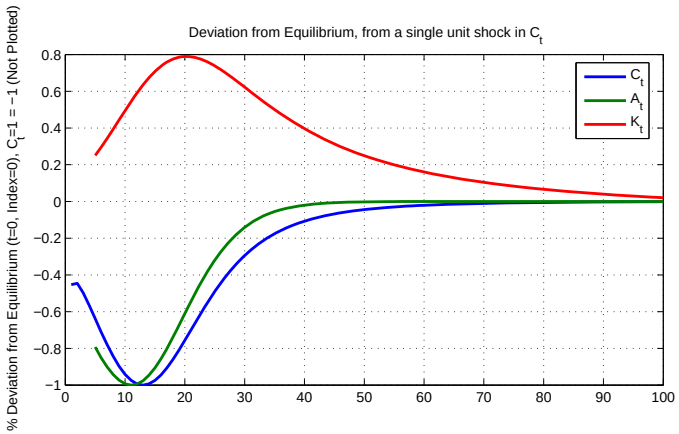
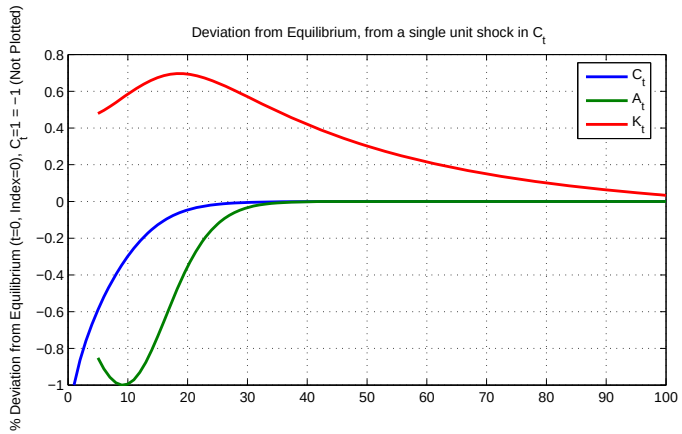
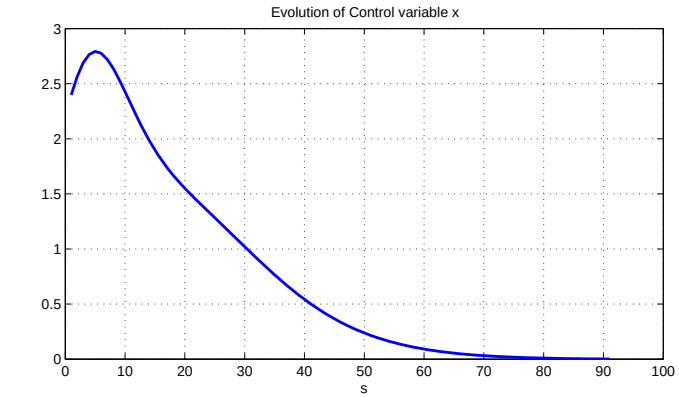


Figure: Impact of Confidentiality Deviations

Example 3: C as Priority







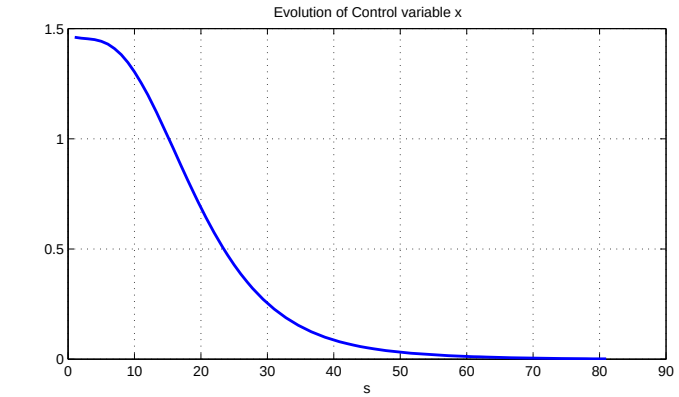


Figure: Level of Vulnerability and Response

Concluding Remarks

- We have presented a framework for evaluating the (relative) consequences of C(I)A preferences based on quadratic loss functions.
- The system is described by a set of differential equations describing the time evolution of the system,
- One time shocks are applied and the impulse response structures computed.
- The model is very flexible and easily parameterized using an MLE or GMM type routine.

Future Research Directions

We envisage a multitude of research directions from this initial treatment.

1. In IPW (2009b) we look at vulnerability management and timing, treating vulnerability shocks to C&A as part of a Doubly Stochastic-Cox type process.
2. We look at Generalising the control problem to an any dimension log-linear vector process, IPW 2009c, this negates the need to formalize C(I)A.
3. Applying discontinuities in the controls and responses.