

The cyber threat Prevention and prosecution

Henry Harrison

21st October 2009

EGV210D012v1.0

The future

- “The future is already here.
It’s just not widely distributed yet”
 - *William Gibson, originator of the term “cyberspace”*

Strong cyber security techniques

Tried and tested techniques

- Strongly separated systems
- Formal methods
- Secure design principles
- Dedicated hardware platforms

New techniques

- Whitelisting
- Trusted Computing
- Hardware virtualisation
- Behavioural anomaly detection

The future

- “The future is already here.
It’s just not widely distributed yet”
 - *William Gibson, originator of the term “cyberspace”*
- “Prediction is very difficult,
especially about the future”
 - *Niels Bohr, father of quantum mechanics*

Risk analysis is difficult and people are bad at it

The senior tranche's notional I_t^{SM} is defined by the relationship

$$I_t^{SM} + \sum_{m=1}^{M-1} I_t^{SM, \Delta_m} = 1 - d_t \quad (\text{Senior tranche loss})$$

The above relationship is necessary to maintain the balance between the coupon cashflow from the underlying portfolio and the payments to the tranches. For example, consider the first default in the underlying portfolio. Some notional n_i defaults and no longer generates coupon. According to the formula (Tranche loss) the equity tranche covers the loss $(1 - R)n_i$ and the notional of the equity tranche decreases by $(1 - R)n_i$. However, the entire portfolio's notional decreases by n_i . Hence, the senior tranche is equipped with the rule that that tranche's notional decreases by Rn_i when the equity and mezzanine tranches are taking losses. Let us confirm that the formula (Senior tranche loss) indeed has such effect.

$$\begin{aligned} I_t^{SM} &= 1 - d_t - \sum_{m=1}^{M-1} I_t^{SM, \Delta_m} = 1 - \sum_j n_j 1_{\{r_j < \alpha_j\}} - \sum_{m=1}^{M-1} \overbrace{(b_m - a_m - I_t^{SM, \Delta_m})}^{-d_t} \\ &= 1 - \sum_j n_j 1_{\{r_j < \alpha_j\}} - \frac{\sum_{m=1}^{M-1} (b_m - a_m)}{b_{M-1}} + \sum_{m=1}^{M-1} \overbrace{[(l_t - a_m)_+ - (l_t - b_m)_+]}^{-l_t - (l_t - b_{M-1})_+} \\ &= 1 - \sum_j n_j 1_{\{r_j < \alpha_j\}} - b_{M-1} + l_t - (l_t - b_{M-1})_+ \\ &= \begin{cases} 1 - \sum_j n_j 1_{\{r_j < \alpha_j\}}, & J_t > b_{M-1} = a_{M, \infty} \\ 1 - \sum_j n_j 1_{\{r_j < \alpha_j\}} - b_{M-1} + l_t, & J_t < a_M. \end{cases} \end{aligned}$$

The $l_t > a_M$ represents the situation when the senior tranche is the only remaining tranche and it covers the entire loss. The $l_t < a_M$ case allows further transformation

“Citigroup’s boss reportedly learned of his organisation’s \$43bn of toxic assets only in September 2007”

“UBS’s post mortem found that ‘at no stage’ did managers have a decent assessment of its subprime exposure”

Source: The Economist, October 2009

Risk analysis in cyber space is especially hard

- **Bug exposes eight years of Linux kernel**

14th August 2009

Linux developers have issued a critical update for the open-source OS after researchers uncovered a vulnerability in its kernel that puts most versions built in the past eight years at risk of complete takeover.

...

This is the second time in less than a month that a serious security vulnerability has been reported in the Linux kernel. In mid July, a researcher alerted Linux developers to a separate NULL pointer dereference bug that put newer versions at risk of complete compromise.

Costing the risk

The senior tranche's notional I_t^{SM} is defined by the relationship

$$I_t^{SM} + \sum_{m=1}^{M-1} I_t^{SM, b_m} = 1 - d_t \quad (\text{Senior tranche loss})$$

The above relationship is necessary to maintain the balance between the coupon cashflow from the underlying portfolio and the payments to the tranches. For example, consider the first default in the portfolio. Some notional n_i defaults and no longer generates coupon. According to the formula (Tranche loss) the equity tranche covers the $(1-R)n_i$ and the notional of the equity tranche decreases by $(1-R)n_i$. However, the entire portfolio notional decreases by n_i . Hence, the senior tranche is equipped with the rule that its notional decreases by Rn_i when the equity and mezzanine tranches are taking losses. Let us confirm that the formula (Senior tranche loss) indeed has such effect.

$$\begin{aligned} I_t^{SM} &= 1 - d_t - \sum_{m=1}^{M-1} I_t^{SM, b_m} = 1 - \sum_j n_j 1_{\{r_j < \alpha\}} - \sum_{m=1}^{M-1} \overbrace{\left(b_m - a_m - I_t^{SM, b_m} \right)}^{-I_t^{SM, b_m}} \\ &= 1 - \sum_j n_j 1_{\{r_j < \alpha\}} - \overbrace{b_M}^{b_M} + \sum_{m=1}^{M-1} \overbrace{\left[(I_t - a_m)_+ - (I_t - b_m)_+ \right]}^{-I_t - (I_t - b_{M-1})_+} \\ &= 1 - \sum_j n_j 1_{\{r_j < \alpha\}} - b_{M-1} + I_t - (I_t - b_{M-1})_+ \\ &= \begin{cases} 1 - \sum_j n_j 1_{\{r_j < \alpha\}}, & J_t > b_{M-1} = a_M \\ 1 - \sum_j n_j 1_{\{r_j < \alpha\}} - b_{M-1} + I_t, & J_t < a_M \end{cases} \end{aligned}$$

The $I_t > a_M$ represents the situation when the senior tranche is the only remaining tranche and it covers the entire loss. The $I_t < a_M$ case allows further transformation

“Measure with a laser

Mark with chalk

Cut with an axe”

An alternative approach

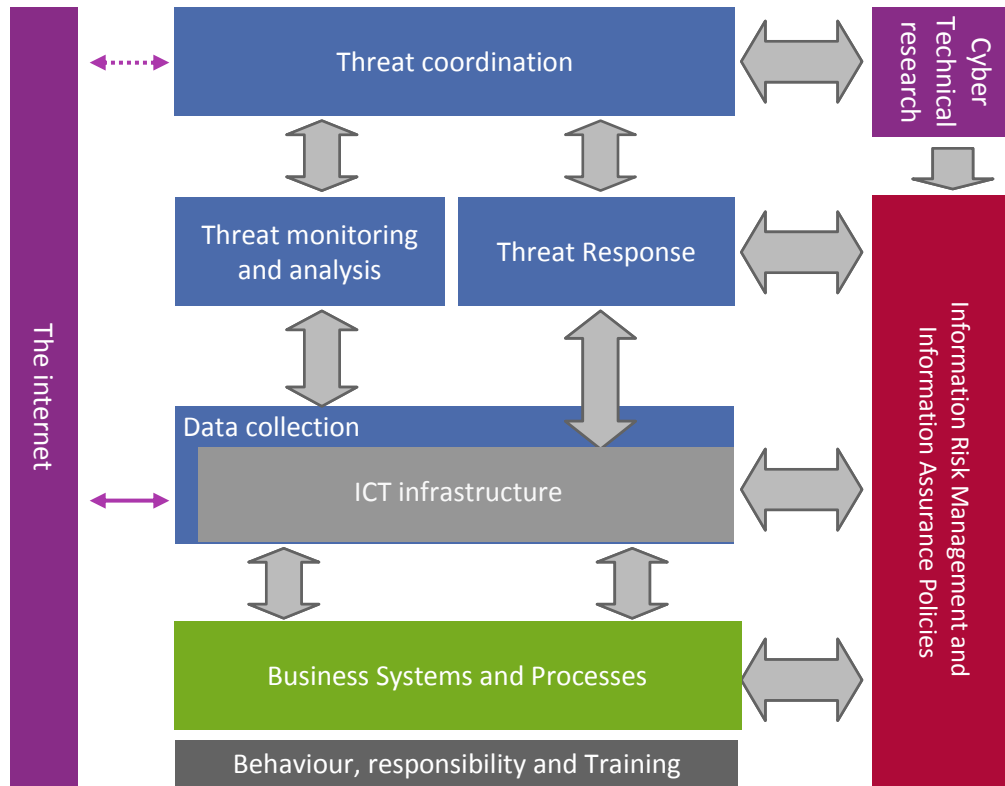
**“Measure by inspection,
mark by eye,
cut with an axe”**

Then measure again, to see what we got wrong

Mark, cut

And keep repeating

Operational model for cyber security



Re-phrasing
the problem:

From risk
reduction to
increased
agility

The future

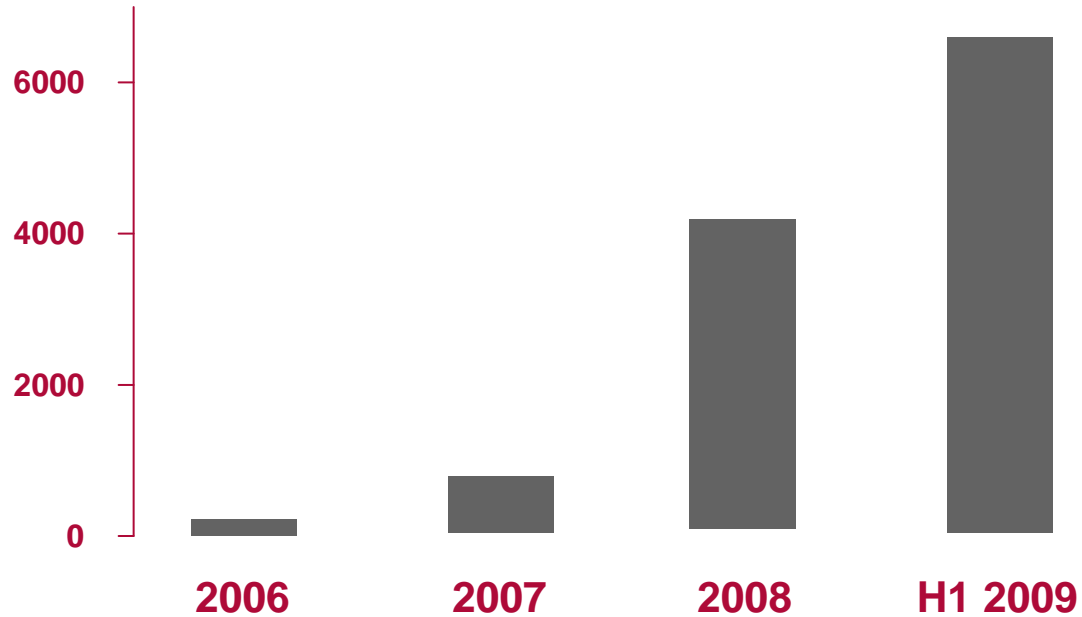
- “The future is already here.
It’s just not widely distributed yet”
 - *William Gibson, originator of the term “cyberspace”*
- “Prediction is very difficult,
especially about the future”
 - *Niels Bohr, father of quantum mechanics*
- “The best way of predicting the future
is to invent it”
 - *Alan Kay, inventor of the modern Graphical User Interface*

Understanding information risk?



Unique new malware

Unique new
malware
variants
discovered
per day



Source: McAfee

Who?

Where?

Society's advantage



Society's advantage...?



Gohardasht Prison Karaj, Iran

Having it both ways?

- The freedom of a flexible cyber space
- The security of a policed cyber space

**The ability to choose based on a
balance of risk**

Contact details

Henry Harrison
Technical Director

henry.harrison@detica.com

T +44 (0)7736 675484

Head Office

Surrey Research Park
Guildford
Surrey
GU2 7YP
UK

Tel: +44 (0)1483 816000

Fax: +44 (0)1483 816144

Arundel Street Office

Arundel Great Court
2 Arundel Street
London
WC2R 3AZ
UK

Tel: +44 (0)20 7812 4000

Fax: +44 (0)20 7812 4100

