A New Resilience Framework

Marcus Thompson
Mike Ryan
Jill Slay
Alan McLucas

UNSW AUSTRALIA

Capability Systems Centre
UNSW Canberra

Introduction

- Whether preserving the availability of a bank balance, ensuring personal safety, preserving the confidentiality of information in a database, or safeguarding the integrity of a territorial border, the aim of security is to maintain the nominated state of a designated resource.
- For that state to be maintained in the presence of agile threats, the security system must be equally agile.
- Such agility requires a framework of agile system components with well-known interactions and the application of agile governance procedures.

Introduction

- Despite security methods being proposed by many national governments, standards organisations, and think tanks, none has achieved a lasting impact.
- Part of the reason for this is that current methods use or rely upon terminology that is confusing, inconsistent, incomplete, or contains language that is specific to the physical, personnel, or electronic domains of security.
- Consequently, the current set of security terms and definitions:
  - provide little assistance in the design and application of security systems
  - do little to provide the firm base necessary for agile security systems that must survive in an environment of uncertainty, unpredictability, and evolution.

Introduction

- This paper presents a security framework based on a harmonised taxonomy of security, resilience and governance that is applicable across the physical, personnel, and electronic domains.
- The utility of the framework is demonstrated for the design of sustainably secure systems and, in particular, for recognition of the essential role played by governance in the provision of agility.

Taxonomy for Security

- A suitable framework for addressing sustainably secure systems is based on harmonised taxonomies of security and resilience. Thompson et al (2012 and 2015), define security as:

Security is the maintenance of the nominated state of a designated resource.

- where the *nominated state* is a specific condition that is determined through a governance process that assesses the intrinsic value of the resource that is *designated* as requiring security, such as an object, entity or data.

Taxonomy for Security

- The definition of security can be elaborated to be:

The security of the nominated state of a designated resource is maintained if and only if an authenticated entity is known to perform an action that is accessible.

- It follows that *authentication*, *attribution* and *access control* are appropriate security services that can be delivered by the application of security mechanisms.
- The full elaboration of the taxonomy of security is supported by a hierarchy of security services and security mechanisms.

Taxonomy for Security

The nominated state of a designated resource is secure if and only if …			
	an authenticated entity	*is known to perform*	*an action that is accessible.*
Security Services	Authentication	Attribution	Access Control
Example Security Mechanisms	Passwords Biometrics Identity Cards Passports Pattern of life analyses Introduction Physical recognition	Notarization Digital Signatures Logging Observation Inspections Recordings Registers	Encryption Permission Controls Validation Firewalls Data Filters Routing Control Proxy Servers Access Lists Visas

Taxonomy for Resilience

- Resilience has application after a security breach—after security has failed. The aim of resilience is to maintain a particular state of security for a designated resource:

  Resilience is the maintenance of the nominated state of security.

- where, the *nominated state* is a specific condition that is determined through a governance process that assesses the intrinsic value of the *designated* resource.
- *Security* is breached once the nominated state of the resource has been changed, and *resilience* is the ability to redress that change to maintain the nominated state – that is, to restore the nominated state of security.

Taxonomy for Resilience

- The definition of resilience can be completely elaborated to be:

  Resilience is maintained if and only if a security breach is detected, contained and resolved.

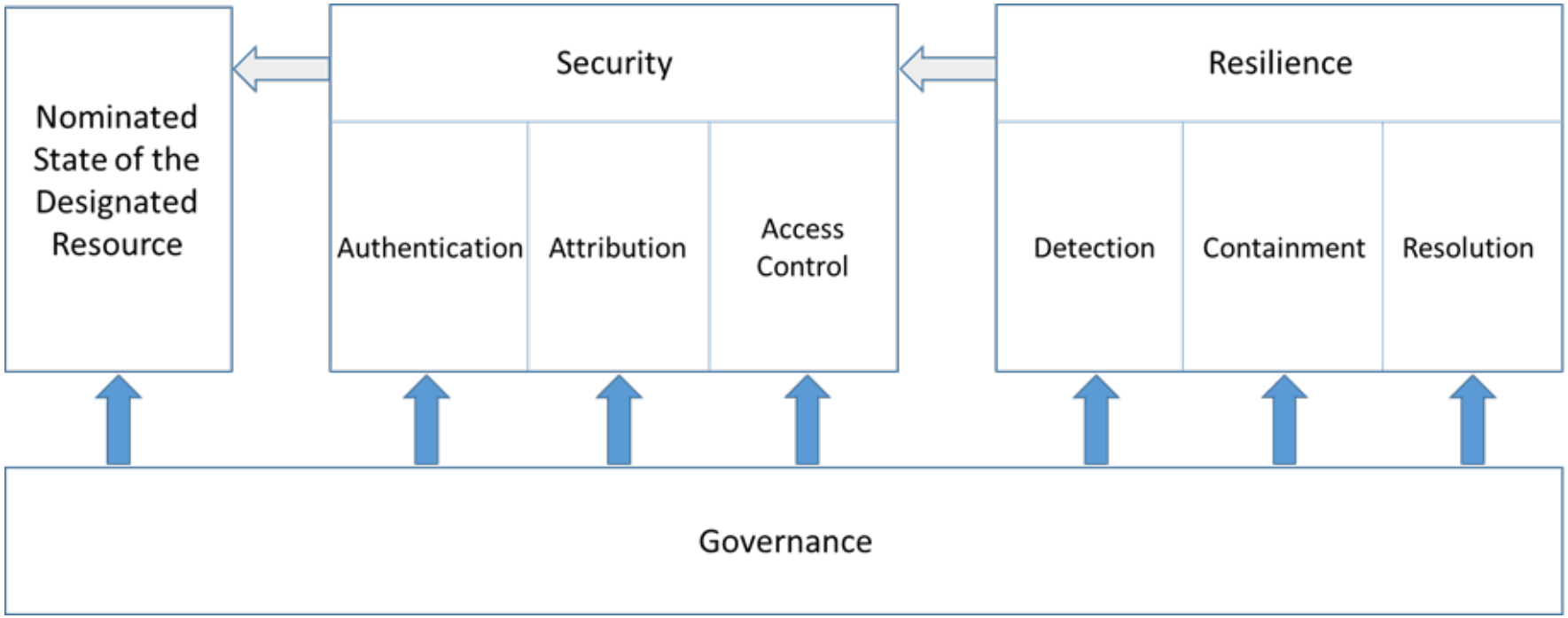
- Since resilience is maintained when a security breach is detected, contained and resolved, it follows that *detection, containment,* and *resolution* are appropriate resilience services.
- The full elaboration of the taxonomy of resilience is supported by a hierarchical resilience taxonomy of definitions supported by resilience services and resilience mechanisms.

Taxonomy for Resilience

Resilience is maintained if and only if a security breach is …			
	detected,	*contained,*	*and resolved.*
Resilience Services	Detection	Containment	Resolution
Resilience Mechanisms	Recognition Identification	Absorption Survivability Impact Limitation	Eradication Restoration

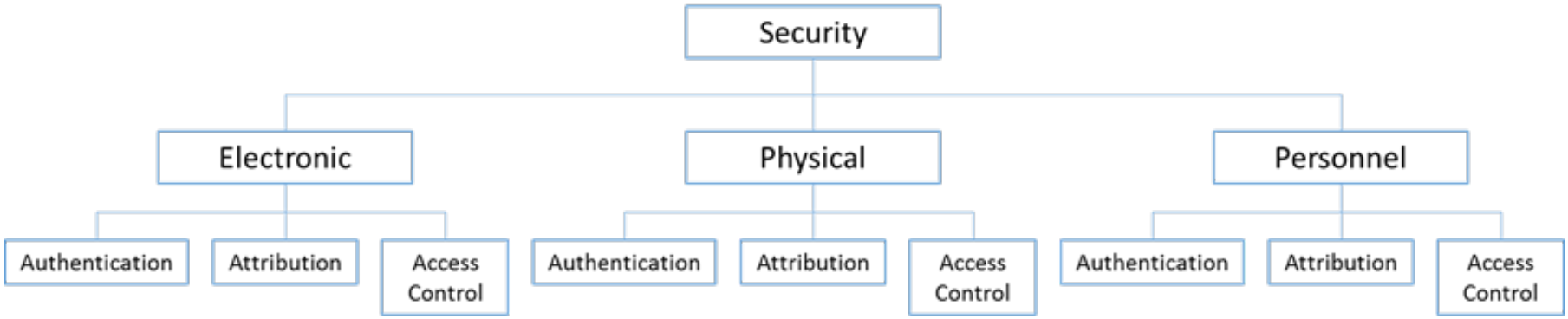
Governance

- Setting or establishing levels of authentication, attribution, and accessibility; and detection, containment and resolution, are specific governance functions that are set based upon an organisation's specific circumstances.



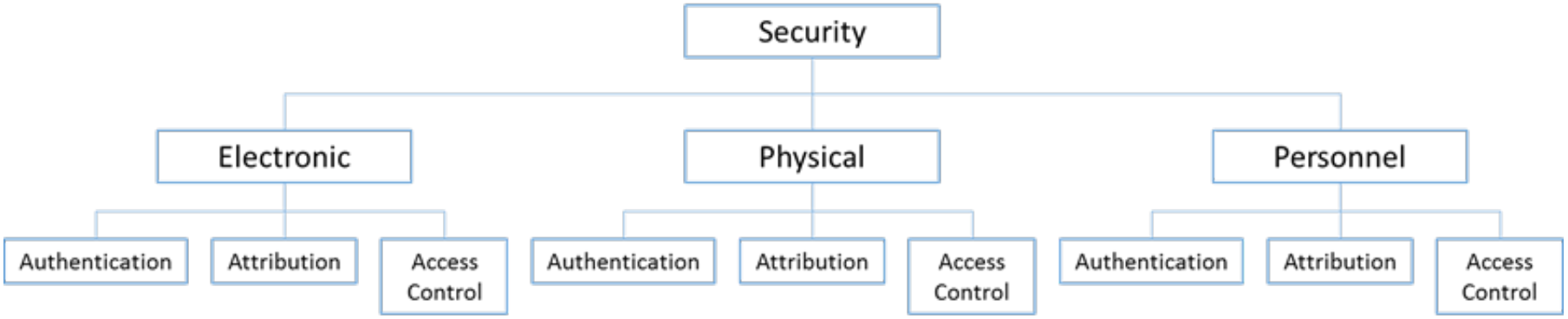
Optimising Security Services

- Traditional views of security governance have focused on three domains—*physical*, *personnel*, and *electronic*—each of which has its own language and nomenclature.



- Resources would be allocated by domain, and domain security managers would deliver authentication, attribution and access control services within their respective domains.
- However, any security system that focuses on a single domain is not adequate.

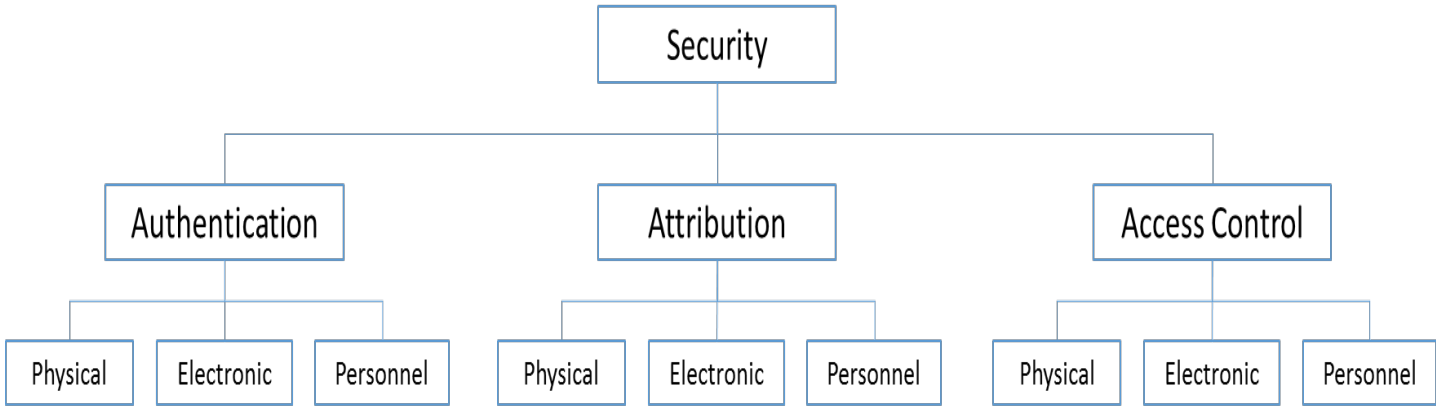
Optimising Security Services



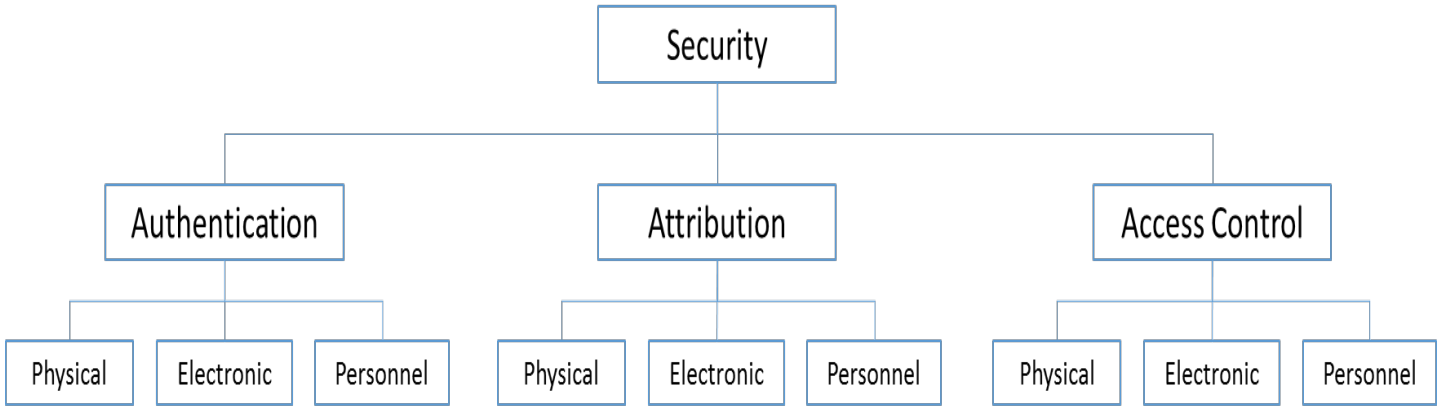
- Optimising a particular security service is not possible in this construct as each security service is considered from a domain-specific view, rather than from a holistic security view.
- Additionally, it is not normally possible to optimise a system by optimising its constituent parts, or sub-systems.

Optimising Security Services

- However, a service-centric perspective of security would recognise domain-specific security requirements, but consists of only one authentication service, one attribution service, and one access control service. This enables a collaborative approach to each of the physical, personnel, and electronic domains.



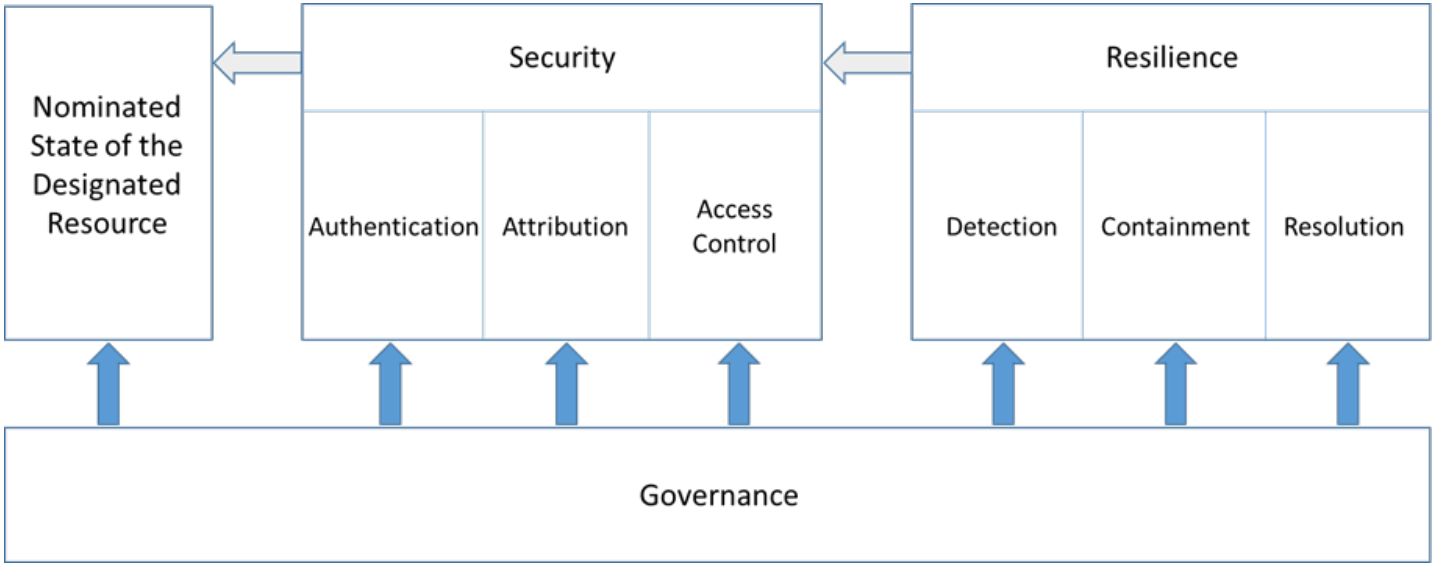
Optimising Security Services



- More importantly, the service-centric security model facilitates the agile application of governance functions to allocate resources to best achieve and/or maintain the nominated state of security. By contrast however, in the domain-centric model, the electronic, physical, and personnel aspects must be balanced meaning that there is no inherent advantage to placing additional emphasis on any one domain than there is on the other domains.

Governance for Sustainable Security

- The significant observation from the framework, which is often only mentioned in passing in many security methodologies, is the critical role that governance plays in the designation of the resource, the nomination of the state of security, the identification of threats to that security, and the judicious selection of security and resilience services to address those threats.



Governance for Sustainable Security

- For a security to be maintained, the nominated state of a designated resource must be maintained in the presence of threats.
- The framework highlights how, having set security and resilience services for an expected level of threat, governance processes might monitor any changes in threat and respond by adjusting the balance of services as appropriate.
- If the threats are agile, then it follows that the security system must be agile in response through agility in the established security services and resilience services which, in turn, requires agile governance.

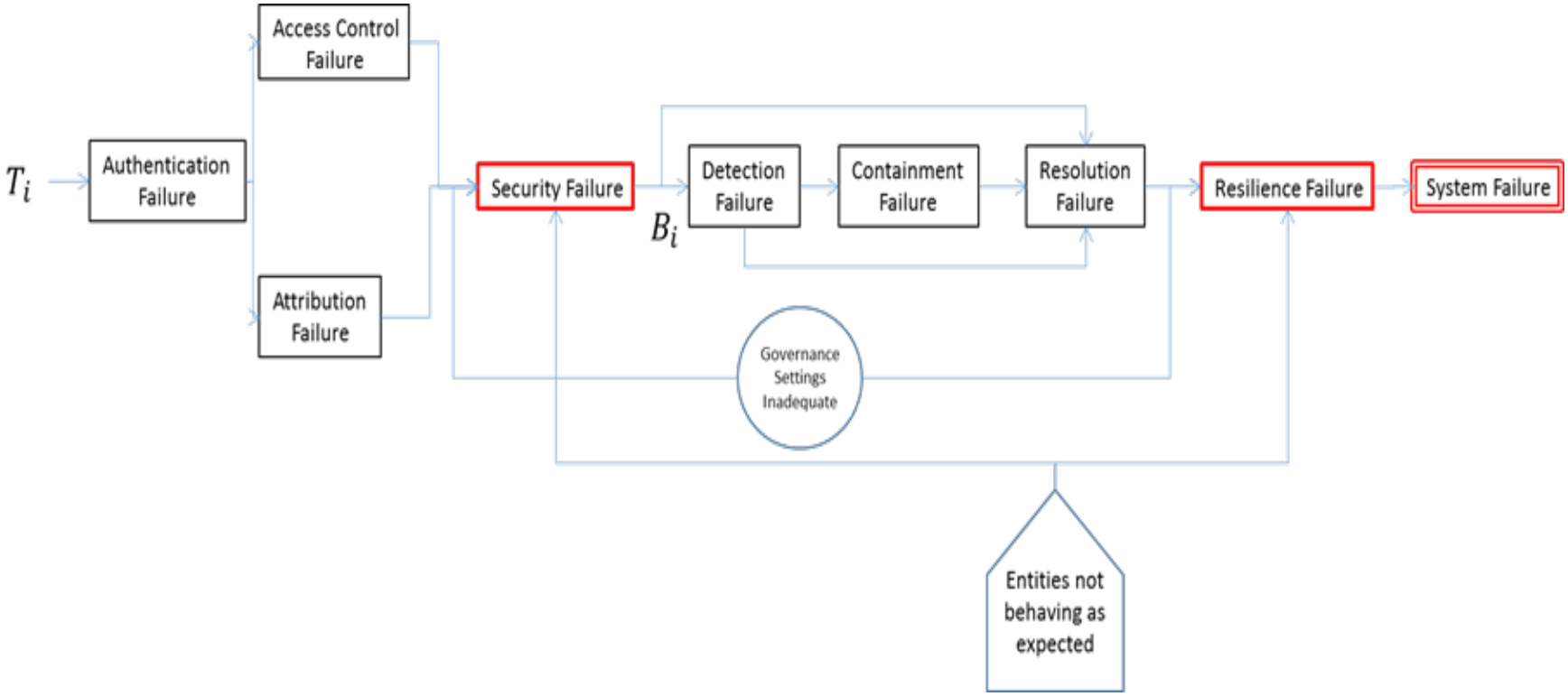
Governance for Sustainable Security

- Even in the presence of constant threats, however, sustainable security requires the adoption of agile governance procedures which must monitor to ensure that the selected security and resilience services remain appropriate.
- Agile governance is required since the correct functioning of security and resilience services relies on all entities acting in the manner expected of them.
- This means that the services must perform within the margins expected of them—that is, each service will rely on at least one mechanism that is expected to have a probability of failure that was specified as part of the design of the security system.

Governance for Sustainable Security

- The failure of a mechanism has two root causes:
  - The technology behind the entity providing the mechanism will have an underlying failure rate because no mechanism is likely to be considered to be foolproof.
  - The entity itself could fail due to such issues as a faulty component or a power failure.
- The first failure rate is set by governance process as the balanced combination of services is selected when the security system is established.
- The second failure rate must be addressed by ongoing agile governance throughout the system's lifecycle.

Governance for Sustainable Security



A Governance Case Study

- The correct operation of entities extends beyond technology to the humans involved.
- For example, consider the 2010 leaking of ‘more than 700,000 classified documents’ from US military networks by then Corporal Bradley Manning (Lewis 2013).
  - As Manning was well known to his colleagues and chain of command, the failure to maintain confidentiality was not a failure of *authentication*.
  - Similarly, it can be assumed that activity on a classified military network was logged, so the incident was not a failure of *attribution*.
  - Further, Manning was an insider who had been granted access, so the incident was not a failure of the *access control* service as it has been originally established.

A Governance Case Study

- However, as an individual who had exhibited questionable behavioural traits, Manning's chain of command should have recognised the need to limit his access permissions, and triggered an appropriate vetting review.
- Rather than represent a failure of any of the security services, the Manning incident represents a failure of *governance*.
- It is misleading to mislabel the lapse as one of a failure of the security services.
- The taxonomies and the associated framework presented earlier greatly assist in avoiding the confusion.

Conclusion

- A harmonised taxonomy of security and resilience is essential to the establishment of a suitable framework necessary for engineering of sustainably secure systems.
- For the nominated state of a designated resource to be maintained in the presence of agile threats, then the security system must be equally agile.
- Although the agility of security and resilience services is clearly important, the use of an appropriate framework identifies that agile security is fundamentally predicated upon the application of agile governance.

Conclusion

- The role of agile governance in sustainably secure systems is twofold:
  - When threats are constant, security must be maintained by ensuring that established security and resilience services are acting as expected.
  - Security and resilience services must be adjusted as required in order to provide agile responses to agile threats.

A New Resilience Framework

Marcus Thompson
Mike Ryan
Jill Slay
Alan McLucas

UNSW AUSTRALIA

Capability Systems Centre
UNSW Canberra