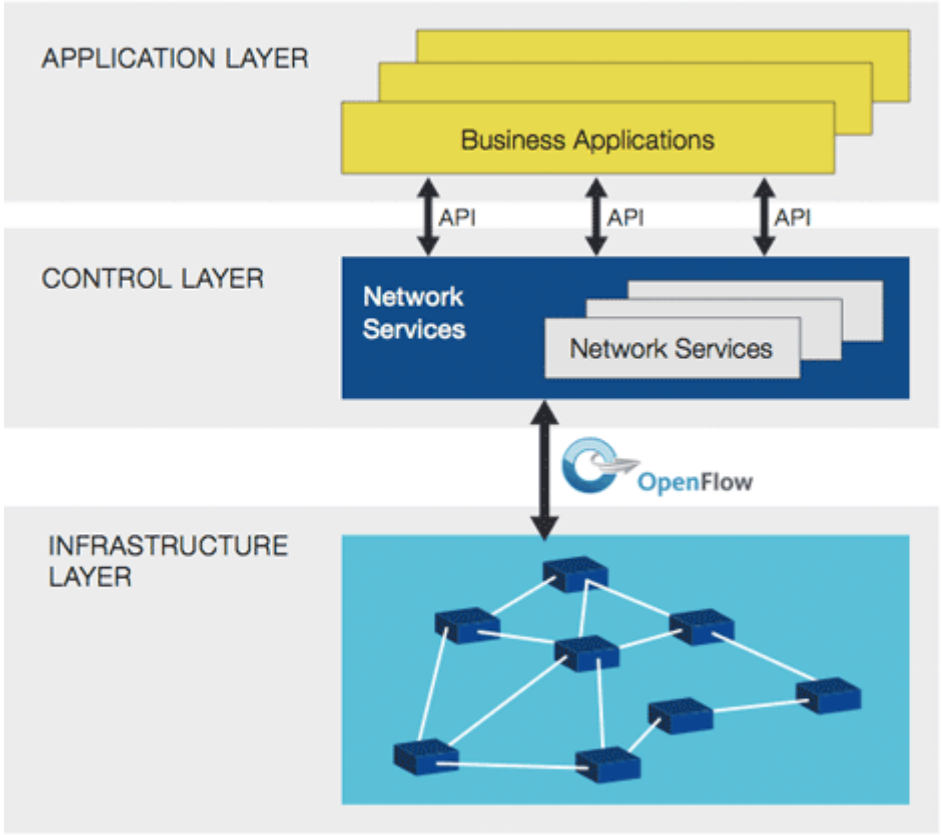
IEEE SDN Initiative
Standardization Committee Meeting
Security Considerations & Concerns

Anton Kaska BTNE, LLC

June 23, 2015 Piscataway, NJ

What are we facing?



ONF Model

ONF SAYS:

Computing Trends are driving network change…

1. *Changing Traffic Patterns*
2. *Consumerization of IT*
3. *Rise of Cloud Services*
4. *Big Data=More Bandwidth*

Constraints listed include:

- *Complexity leads to stasis*
- *Inability to scale*
- *Vendor Dependence*

WHAT IS INDUSTRY SAYING?

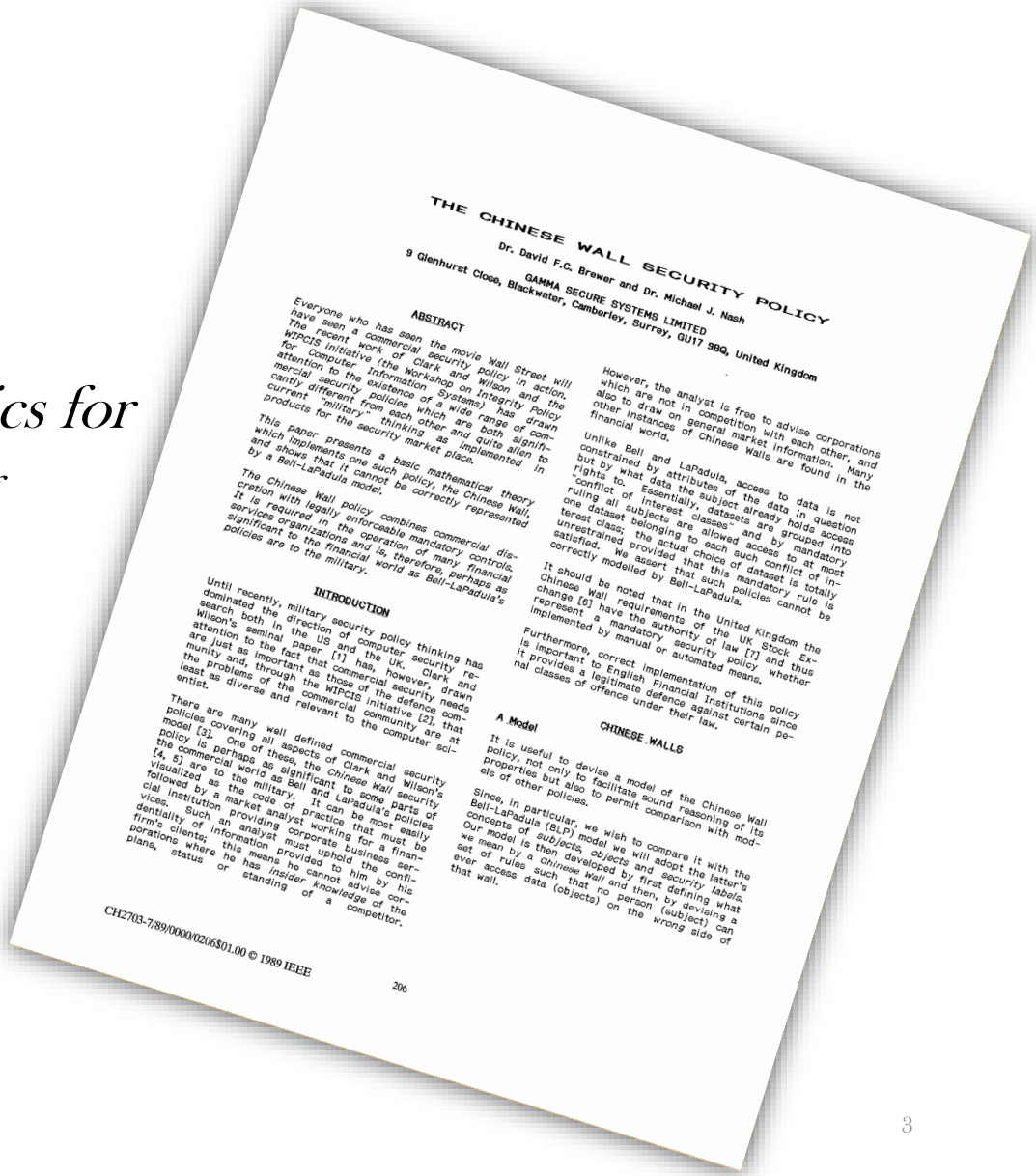
1. *The same approach*
2. *The same architecture*
3. *The same security drivers*

…not quite

Not a new challenge we are facing

Defense in Depth with specifics for Software Defined Networking

- ✓ *Baseline Security Models*
- ✓ *Integrity Checks*
- ✓ *Brewer-Nash Model?*
- ✓ *Physical Security*



THE CHINESE WALL SECURITY POLICY

Dr. David F.C. Brewer and Dr. Michael J. Nash
GAMMA SECURE SYSTEMS LIMITED
9 Glenhurst Close, Blackwater, Camberley, Surrey, GU17 9BQ, United Kingdom

ABSTRACT

Everyone who has seen the movie Wall Street will have seen a commercial security policy in action. The recent work of Clark and Wilson and the WIPCIS initiative (the Workshop on Integrity Policy for Computer Information Systems) has drawn attention to the existence of a wide range of commercial security policies which are both significantly different from each other and quite alien to current "military" thinking as implemented in products for the security market place.

This paper presents a basic mathematical theory which implements one such policy, the Chinese Wall, and shows that it cannot be correctly represented by a Bell-LaPadula model.

The Chinese Wall policy combines commercial discretion with legally enforceable mandatory controls. It is required in the operation of many financial services organizations and is, therefore, perhaps as significant to the financial world as Bell-LaPadula's policies are to the military.

INTRODUCTION

Until recently, military security policy thinking has dominated the direction of computer security research both in the US and the UK. Clark and Wilson's seminal paper [1] has, however, drawn attention to the fact that commercial security needs are just as important as those of the defence community and, through the WIPCIS initiative [2], are at the problems of the commercial community are at least as diverse and relevant to the computer scientist.

There are many well defined commercial security policies covering all aspects of Clark and Wilson's model [3]. One of these, the *Chinese Wall* security policy is perhaps as significant to some parts of the commercial world as Bell and LaPadula's policies are to the military. It can be most easily visualized as the code of practice that must be followed by a market analyst working for a financial institution providing corporate business services. Such an analyst must uphold the confidentiality of information provided to him by his firm's clients; this means he cannot advise corporations where his *insider knowledge* of a competitor's status or standing of a plans,

However, the analyst is free to advise corporations which are not in competition with each other, and also to draw on general market information. Many other instances of Chinese Walls are found in the financial world.

Unlike Bell and LaPadula, access to data is not constrained by attributes of the data in question but by what data the subject already holds access rights to. Essentially, datasets are grouped into "conflict of interest classes" and by allowed access to at most one dataset subjects are allowed access to each such conflict of interest class; the actual choice of dataset is totally unrestrained provided that this mandatory rule is satisfied. We assert that such policies cannot be correctly modelled by Bell-LaPadula.

It should be noted that in the United Kingdom the Chinese Wall requirements of the UK Stock Exchange [6] have the authority of law [7] and thus represent a mandatory security policy whether implemented by manual or automated means.

Furthermore, correct implementation of this policy is important to English Financial Institutions since it provides a legitimate defence against certain penal classes of offence under their law.

CHINESE WALLS

A Model

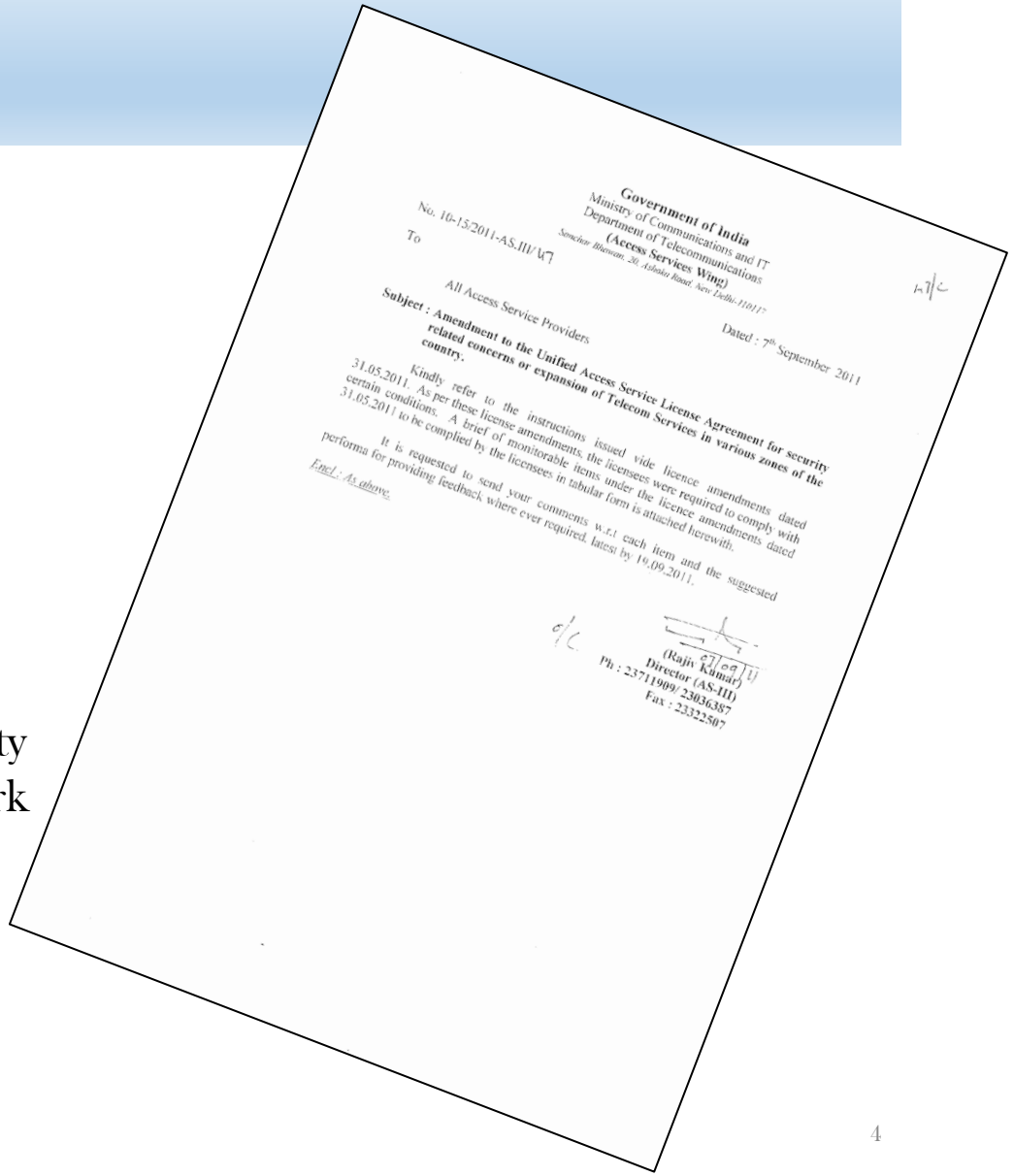
It is useful to devise a model of the Chinese Wall policy, not only to facilitate sound reasoning of its properties but also to permit comparison with models of other policies.

Since, in particular, we wish to compare it with the Bell-LaPadula (BLP) model we will adopt the latter's concepts of *subjects*, *objects* and *security labels*. Our model is then developed by first defining what we mean by a *Chinese Wall* and then, by devising a set of rules such that no person (subject) can ever access data (objects) on the wrong side of that wall.

How do we accomplish and not fail (PCI, ETSI, IEEE, etc?

Bundesamt für Sicherheit in der Informationstechnik

BSI-Standard 100-2:IT-Grundschutz Vorgehensweise



Government of India
Ministry of Communications and IT
Department of Telecommunications
(Access Services Wing)
Sanchar Bhawan, 20, Ashoka Road, New Delhi-110001

No. 10-15/2011-AS.III/47

To

All Access Service Providers

Dated : 7th September 2011

Subject : Amendment to the Unified Access Service License Agreement for security related concerns or expansion of Telecom Services in various zones of the country.

Kindly refer to the instructions issued vide licence amendments dated 31.05.2011. As per these license amendments, the licensees were required to comply with certain conditions. A brief of monitorable items under the licence amendments dated 31.05.2011 to be complied by the licensees in tabular form is attached herewith.

It is requested to send your comments w.r.t. each item and the suggested performa for providing feedback where ever required, latest by 16.09.2011.

Encl.: As above.

(Rajiv Kumar)
Director (AS-III)
Ph : 23711909/ 23036387
Fax : 23322507

3 GPP

TS 33.210TS Network Domain Security
TS 33.310 Authentication Framework
TS 33.401 Security Architecture

A Flexible Model

THE CHINESE WALL SECURITY POLICY

Dr. David F.C. Brewer and Dr. Michael J. Nash

GAMMA SECURE SYSTEMS LIMITED
9 Glenhurst Close, Blackwater, Camberley, Surrey, GU17 9BQ, United Kingdom

ABSTRACT

Everyone who has seen the movie Wall Street will have seen a commercial security policy in action. The recent work (the Workshop on Integrity Policy for Computer Systems) has drawn attention to the existence of a wide range of commercial security policies which are both significantly different from each other and quite alien to current "military" thinking as implemented in products for the security market place.

This paper presents a basic mathematical theory which implements one such policy, the Chinese Wall, and shows that it cannot be correctly represented by a Bell-LaPadula model.

The Chinese Wall policy combines commercial discretion with legally enforceable mandatory controls. It is required in the operation of many financial services organizations and is, therefore, perhaps as significant to the financial world as Bell-LaPadula's policies are to the military.

INTRODUCTION

Until recently, military security policy thinking has dominated the direction of computer security research both in the US and the UK. Clark and Wilson's seminal paper [1] has, however, drawn attention to the fact that commercial security needs are just as important as those of the defence community and, through the WIPCIS initiative [2], that the problems of the commercial community are at least as diverse and relevant to the computer scientist.

There are many well defined commercial security policies covering all aspects of Clark and Wilson's model [3]. One of these, the Chinese Wall security policy is perhaps as significant to some parts of the commercial world as Bell and LaPadula's policies are to the military. It can be most easily visualized as the code of practice that must be followed by a market analyst working for a financial institution providing corporate business services. Such an analyst must uphold the confidentiality of information provided to him by his firm's clients; this means he cannot advise on operations where he has insider knowledge of the plans, status or standing of a competitor.

However, the analyst is free to advise corporations which are not in competition with each other, and also to draw on general market information. Many other instances of Chinese Walls are found in the financial world.

Unlike Bell and LaPadula, access to data is not constrained by attributes of the data in question but by what data the subject already holds access rights to. Essentially, datasets are grouped into "conflict of interest classes" and by mandatory ruling all subjects are allowed access to at most one dataset belonging to each such conflict of interest class; the actual choice of dataset is totally unrestrained, provided that this mandatory rule is satisfied. We assert that such mandatory policies cannot be correctly modelled by Bell-LaPadula.

It should be noted that in the United Kingdom Chinese Wall requirements of the UK Stock change (6) have the authority of law [7] and represent a mandatory security policy implemented by manual or automated means.

Furthermore, correct implementation of th is important to English Financial Institut it provides a legitimate defence against nal classes of offence under their law.

CHINESE WALLS

A Model

It is useful to devise a model of policy, not only to facilitate proper properties but also to permit co els of other policies.

Since, in particular, we wish Bell-LaPadula (BLP) model we Our model is then develope we mean by a Chinese Wal set of rules such that ever access data (ob that wall.

200

CH2703-7/89/0000/0206$01.00 © 1989 IEEE

Remember Physical Security

Summary

- Multiple attempts at security ***Standards*** but focused on verticals, size, business models, point technologies, etc.
- Using security as it has been practically applied, as a historical illustration
  - we will not meet the challenges sufficiently
  - there are many examples to glean knowledge from.
- A flexible approach is required.
- Given the speed with which technology advances, leveraging existing best practices and solutions that have proven themselves (Defense in Depth Theory, Chinese Walls, etc.) will provide acceptable and **practical** levels of mitigation that are implementable with tolerable financial and political cost.
- A more complex matrixes approach leveraging industry specific and/or business requirement based risk mitigation is likely a requirement when viewed long term
  - This is in my opinion the harder nut to crack for the industries as a whole (and organizations such as IEEE)