



QUESTnet 2008



Do you know and trust your name in cyberspace?

Emeritus Professor William J (Bill) Caelli, AO
IISEC Pty Ltd

and

Information Security Institute,
Queensland University of Technology

(c) W. Caelli - IISEC Pty Ltd

1

Agenda:

- What's in a name?
- Your name – your computer's name
 - Claiming & verifying
- Naming & addressing systems
 - The “DNSSEC” challenge
 - everything.gut - gTLDs

(c) W. Caelli - IISEC Pty Ltd

2

Agenda:

- What's in a name?
- Your name – your computer's name
 - Claiming & verifying
- Naming & addressing systems
 - The “DNSSEC” challenge
 - everything.gut - gTLDs

(c) W. Caelli - IISEC Pty Ltd

3

The Naming of Cats

The Naming of Cats is a difficult matter,
It isn't just one of your holiday games;
You may think at first I'm as mad as a hatter
When I tell you, a cat must have
THREE DIFFERENT NAMES.
(or more for computers)

→ “Computers”

Old Possum's Book of Practical Cats (1939)



(c) W. Caelli - IISEC Pty Ltd



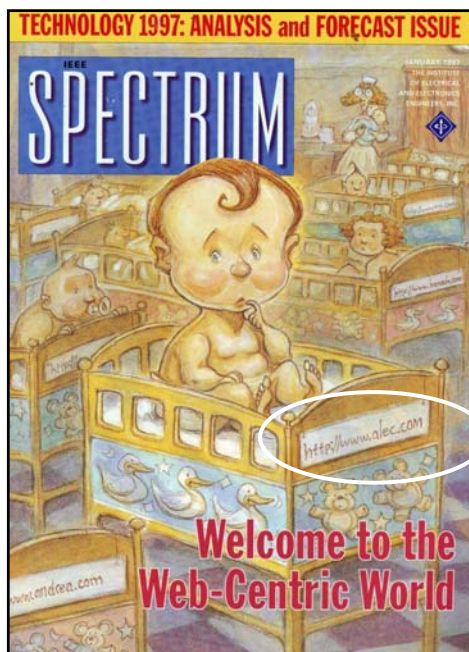
PSTN - POTS

- Your telephone number
- ITU standard
- Country codes
- Number portability
- High trust “exchanges” (switches)
- Force of law
 - Telecoms Acts

Manual exchange, Winnemucca, Nevada – Operated till 1960s

IISEC Pty Ltd

5



IEEE Spectrum

January 1997

*A name in
cyberspace from
birth??*

(c) W. Caelli - IISEC Pty Ltd

6

What's
IN
a
name ?

From: St. George Bank[SMTP:SECURE@STGEORGE.COM.AU]
Sent: Tuesday, May 13, 2008 2:27:32 AM
To: Qut.physicalsc
Subject: Verify Your Phone Number
Auto forwarded by a Rule

Dear customer!

St.George Bank Limited is constantly working to improve the account security of our customers. In order, to ensure the integrity and security of our online banking system, we periodically review accounts. We were unable to contact you by phone during the last check, so please verify the information at your account file and make sure it is right.

Please, verify your account information by following the link.
For personal accounts: <https://ibank.stgeorge.com.au/verify/>
For business accounts: <https://ibank.stgeorge.com.au/bbonline/verify/>

The next verification will be done soon, invalid account information will result in your account being placed to restricted status.

Customer Service
St. George Bank Limited

http://stgeorgebankaustralia.com/

start CA

<https://ibank.stgeorge.com.au/verify>

<http://stgeorgebankaustralia.com>

(c) W. Caelli - IISEC Pty Ltd 7

WATCHING YOUR NAME

Division of Technology, Information and Learning Support

QUT Information Technology Services

4 July 2008

Dear Staff Member

Information Technology Services (ITS) advises all staff that phishing emails are circulating asking for your username and password. These emails use an @qut.edu.au address (abuse.@qut.edu.au) with subject lines such as "Quarantined Account Violation". **DO NOT REPLY** to them.

PGP ??

>15 years ago

Although these emails appear to come from legitimate QUT sources, QUT will never use emails to ask for your username and password!

(c) W. Caelli - IISEC Pty Ltd 8

Agenda:

- What's in a name?
- Your name – your computer's name
 - Claiming & verifying
- Naming & addressing systems
 - The “DNS – Sec” challenge
 - *everything.qut - gTLDs*

(c) W. Caelli - IISEC Pty Ltd

9

- end to end
 - identity
 - authentication
 - authorisation
 - confidentiality



Navajo Code Talkers, Saipan, June 1944



URL: <http://www.navajocodetalkers.org/>

(c) W. Caelli - IISEC Pty Ltd

10

What you know.

- Passwords/passphrases/PINs
 - Absolutely depend upon trusted channel
 - Claimant to/from verifier
- Obsolete with PCs (even Bill Gates)
 - NO trusted channel
- Facebook / social networking
 - End of “*what you know*” – alone.

What you possess – What you are

(c) W. Caelli - IISEC Pty Ltd

11

W Y S I W Y G

NOT



(c) W. Caelli - IISEC Pty Ltd

12

CHALLENGE OF THE TRUSTED CHANNEL

- End – to – end trust requirement
 - NOT just the network (SSL)
 - Microsoft “*Palladium*” project – where ????
 - Intel “La Grande” = VTx / VTd?
 - OS / Middleware / Apps support ?
 - SELinux, Trusted BSD, etc
- Users (human)
 - trust automated process
- Users (processes)
 - SCADA etc

Policy / law:

Computer security
is radically different
to personal/human
user security.

(c) W. Caelli - IISEC Pty L

Agenda:

- What’s in a name?
- Your name – your computer’s name
 - Claiming & verifying
- Naming & addressing systems
 - The “DNS – Sec” challenge
 - *everything.qut - gTLDs*

(c) W. Caelli - IISEC Pty Ltd

14

NeTDevilz



You think that you control the domains but you don't!

Everybody knows wrong.

We control the domains including ICANN!

Don't you believe us?



haha :)

(Lovable Turkish hackers group)

©2008 NetDevilz Co.

We're not first, But We're the BEST!

**AusCERT**
Australian Computer Emergency Response Team

**US-CERT**
UNITED STATES COMPUTER EMERGENCY READINESS TEAM



IMP #1

Interface Message Processor

(Computer History Museum
Mountainview, California, USA)

- separate hardware & firmware
- NOT general purpose
- control & management
- secure from the start
 - DIA RFCs
 - classified
 - compartmentalised
 - prioritised

Honeywell DDP-516

(c) W. Caelli - IISEC Pty Ltd

17



Improve the Security and Resilience of Key Internet Protocols

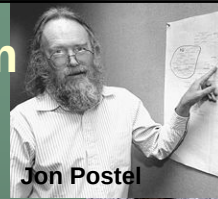
Essential to the security of the Internet infrastructure is ensuring the reliability and secure use of **three key protocols:** the Internet Protocol (IP), the Domain Name System (DNS), and the Border Gateway Protocol (BGP).

(c) W. Caelli - IISEC Pty Ltd

18

DNS - Domain Name System

- New “telephone number systems”
 - DNS servers = telephone exchanges ?
 - “Google” = white pages ?
 - Documentation / training ?
- ICANN & IANA vs CCITT/ITU
 - Role of nation states ?
- DNS - Not designed with any security in mind



Jon Postel



Paul Mockapetris

(c) W. Caelli - IISEC Pty Ltd

19

DNS - Domain Name System

- IPv6 & DNSSec ??
 - Uptake
 - Economics
 - Policy & regulation
- New imperative – FttN / NBN
 - Interaction with “copper” / PSTN exchanges
- New threats – gTLD – “.australia” domain

(c) W. Caelli - IISEC Pty Ltd

20

CONCLUSIONS ?



A Next Generation Networks (NGN) is a packet-based network able to provide Telecommunication Services to users and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent of the underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and services of their choice. It supports generalised mobility which will allow consistent and ubiquitous provision of services to users.

NGN SECURITY

Security is as crucial to the NGN as it is in today's network environment. The very wide scope of this topic, combined with the number of SDOs (standards development organisations) already involved, underlines the strategic importance of this subject. Within the NGN, security issues interrelate with architecture, QoS, network management, mobility, charging and payment.

Security studies in NGN are addressing:

- a comprehensive security architecture for NGNs
- the preparation of NGN operational security policy and guidelines
- NGN security protocols and APIs (application programming interface)

(c) W. Caelli - IISEC Pty Ltd

23

Challenges:

- end to end TRUST
 - naming – identity
 - comms channel
 - DNSSEC / IPv6 uptake ?
- capacity
 - 80% for “YouTube” / entertainment ?
 - video/audio streams vs packet switching

NOTE:

Academic & school systems are PRIME candidates for identity theft attacks

(c) W. Caelli - IISEC Pty Ltd

24

Challenges:

URL: <http://www.cisse.info>

EDUCATION & TRAINING

- massive decline over last 5 years
 - ~50% staff FTE ?
- USA / UK / Australia
 - aging academic population
 - academic expertise / retraining ?
- ICT = games & “*secretarial studies*” ?
- situation recognised as **critical**
- Government response is NOW an URGENT national security requirement

(c) W. Caelli - IISEC Pty Ltd

25

E-Security Review



Australian Government
Department of Broadband,
Communications and the Digital Economy



Australian Government
Attorney-General's Department

Submissions to the E-Security Review close on **31 July 2008**

On 2 July 2008, the Australian Government announced a review into the Government's e-security policy, programs and capabilities.

The purpose of the review is to develop a new Australian Government E-Security Framework in order to create a secure and trusted electronic environment for both public and private sectors.

Senator the Hon Stephen Conroy
Minister for Broadband, Communications
and the Digital Economy



Attorney-General, The Hon
Robert McClelland MP



**S
U
B
M
I
T**

http://www.ag.gov.au/www/agd/agd.nsf/Page/Consultationsreformsandreviews_E-SecurityReview_E-SecurityReview

(c) W. Caelli - IISEC Pty Ltd

26

E-Security Review



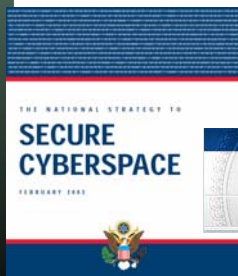
Australian Government
Department of Broadband,
Communications and the Digital Economy



Australian Government
Attorney-General's Department

Submissions to the E-Security Review close on 31
July 2008

Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people.



(c) W. Caelli - IISEC Pty Ltd

27

SOME REFERENCES AND PLACES TO GO:

URLs

www.itu.int International Telecommunications Union

<http://snad.ncsl.nist.gov/dnssec/>

NIST DNSSec Project

<http://www.icann.org/> ICANN - Internet Corporation
for Assigned Names and Numbers

<http://www.iana.org> Internet Assigned Numbers
Authority

<http://www.whitehouse.gov/pcipb/> USA National
Strategy to Secure Cyberspace - 2003

(c) W. Caelli - IISEC Pty Ltd

28

THANK YOU....



BUT

Remember:

Many on the
Gold Coast live in
“broadband poverty”

Telstra

**RIM and Pair Gain
Gaven, Qld.**

~ 35 Kbits/sec

Email:
w.caelli@iisec.com.au

(c) W. Caelli - IISEC Pty Ltd

29