From New Zealand with Fail
DISCLAIMER

FOBSKI and FOSM'S opinions are theirs and theirs alone. They do NOT represent the opinions of their employers, past, present or future. Neither do their opinions constitute professional advice.

This presentation may contain traces of IE6, CISSP, APT and PCI.

NB. No QSAs were harmed during the making of this presentation.
From New Zealand with Faiil
The Fail-abet

with Faily the Fail Monster

and Thought Leader Fobski
A is for....

Apple
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0) {
    goto fail;
} else {
    goto fail;
} 
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0) {
    goto fail;
}

err = sslRawVerify(ctx,
    ctx->peerPubKey,
    dataToSign,
    dataToSignLen,
    signature,
    signatureLen);

if(err) {
    sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify 
    "returned %d\n", (int)err);
    goto fail;
}

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
Nipple unlocks new iPhone

Last updated 12:53 24/09/2013

YouTube

NIPPLEGATE: One man's unusual use of Apple's Touch ID on its new iPhone models.
B is for...

BitCoin
Mo' Money. Mo' Money. Mo' Money.

NO MONEY.
This weekend, there was a *Magic The Gathering* tournament in Richmond, Virginia. It was one of the biggest *Magic* tournaments ever. For posterity's sake, one man set out to record the event in the most memorable possible: with buttcacks.
C is for....

COUNCILS,
CREDIT CARDS,
CARPARKS
and
CONFICKER
NZ asks FBI to help nail hackers

By Jared Savage
4:00 AM Saturday May 1, 2010

The FBI has been asked to help police investigate an international cyber-crime syndicate that hacked into a council-owned carpark to steal credit card details from thousands of customers.

The theft of credit card details from payment machines at the Downtown carpark in central Auckland was discovered in November. It had gone undetected for some time.

Victims of the scam have told the Herald their card details were used to make purchases in Phoenix, Arizona, which suggests the hackers are based overseas.

Car park hack puts credit cards at risk

CHRIS GARDNER Last updated 15:25 08/08/2013

Reports that hundreds of parking machines could be infected with a credit card number harvesting virus are unfounded, the head of Wilson Parking says.

Chief executive Steve Evans said no virus could affect pay-and-display machines, which did not contain a computer like some in Hamilton did.

It was reported today that a compromised machine in Wilson Parking's Alexandra St car park in Hamilton was displaying an error message this week.

The message warned that the machine was infected with the Conficker virus – the same virus that disabled Waikato District Health Board's 3000 computers in 2009.

"I would definitely not put my credit card in this machine or any Wilson Parking machine until I felt confident that the system had been fixed," Aura Information Security managing director Andy Prow told the newspaper.
D was for....

DISTRIBUTE IT
TUESDAY, 21 JUNE 2011

Update, Shared Hosting Clients - 21st June 2011

Our Data Recovery teams have been working around the clock in an attempt to recover data from the affected servers shared Servers. At this time, We regret to inform that the data, sites and emails that were hosted on Drought, Hurricane, Blizzard and Cyclone can be considered by all the experts to be unrecoverable. While every effort will be made to continue to gain access to the lost information from those hosting servers, it seems unlikely that any usable data will can be salvaged from these platforms. In assessing the situation, our greatest fears have been confirmed that not only was the production data erased during the attack, but also key backups, snapshots and other information that would allow us to reconstruct these Servers from the remaining data.

We have been advised by the team and the storage & capacity managers that we no longer have sufficient resources within the platform to transfer the 4,800 domains and accounts to other parts of the platform, and at this point we cannot undertake further provisioning of servers & accounts on the current infrastructure. This leaves us little choice but to assist you in any way possible to transfer your hosting and email needs to other hosting providers. We would like to thank those loyal customers who have stuck by us during this difficult time and elected to have their hosting remain on our servers. Your thoughts, consideration and kindness will not be easily forgotten. Much soul-searching and thought has gone into taking this course of action, but at this time we cannot see any alternatives for the affected servers.
D is for....
Microsoft Gave Google a Copyright Takedown Request for Microsoft.com
(http://gizmodo.com/microsoft-gave-google-a-copyright-takedown-request-for-955659666)
E is for....

EA GAMES
E is for....
EA Games website hacked to steal Apple IDs

An EA Games server has been compromised by hackers and is now hosting a phishing site which targets Apple ID account holders.

The compromised server is used by two websites in the ea.com domain, and is ordinarily used to host a calendar based on WebCalendar 1.2.0. This version was released in September 2008 and contains several security vulnerabilities which have been addressed in subsequent releases. For example, CVE-2012-5385 details a vulnerability which allows an unauthenticated attacker to modify settings and possibly execute arbitrary code. It is likely that one of these vulnerabilities was used to compromise the server, as the phishing content is located in the same directory as the WebCalendar application.
F is for...

FLIGHT CENTRE
Flight Centre's $123k attack by hackers

By Patrice Dougan

Pair accused of accessing Flight Centre computer system for customers' card details.
G is for....
Vladimir Putin accused of spying on world leaders at G20 summit with "poisoned" computer memory sticks

Russia denies spying on G20 leaders at St Petersburg summit

President Putin’s spokesman says allegations are aimed at diverting attention away from controversy over NSA surveillance

Lizzy Davies in Rome
The Guardian, Tuesday 29 October 2013 17.49 GMT
Jump to comments (...)

President Putin at the welcoming ceremony of the G20 summit in St Petersburg in September. Photograph: Sergey Guneev/EPA
Adobe Hacked, 2.9 Million Customer Accounts Compromised

Adobe hack affects 38 million users, not 2.9 million

Number of Adobe Accounts Hacked Now Up to 150M, Check Yours
H is for....

HALF OF KOREA
Nearly HALF of South Korea hacked in insider data theft

Temporary contractor cuffed after credit card swipe

By Phil Muncaster, 20th January 2014
PCI Security Standards Council acknowledges that

**Faily Monster**

has successfully fulfilled the requirements for designation as a

Payment Card Industry Qualified Security Assessor

and has been approved to perform PCI Data Security Assessments in the regions authorized by the PCI SSC on this date

- **April 3rd 2014**

PCI QSA Code: [redacted]

This designation is subject to re-qualification at 12-month intervals and suspension or revocation for failure to comply with any applicable requirement set forth in the current version of the Payment Card Industry (PCI) Data Security Standard Validation Requirements for Qualified Security Assessors.
THIS IS TO ACKNOWLEDGE THAT

Faily Monster

bearing the membership ID ECC928360 for
CEH Version 5.0

HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND
CRITERIA FOR SAID CERTIFICATION THROUGH
EXAMINATION ADMINISTERED BY EC-COUNCIL

EC-Council

December 5, 2008

JAY BAVISI, PRESIDENT

DATE
Defaced again? Yep, good job reusing your passwords morons jack67834#

owned by certified unethical software security professional
Obligatory link: http://attrition.org/errata/charlatan/ec-council/
-Eugene Belford

P.S It seems like lots of you are missing the point here, I'm sitting on thousands of passports belonging to LE (and .mil) officials

FW: CEH Eligibility Application - request for exam code (Pearson Vue)

Snowden, Edward J CTR USAF PACAF DSJR/DSJR <edward.snowden.ctr@yokota.af.mil>

To: cehapp
From: Snowden, Edward J CTR USAF PACAF DSJR/DSJR
Sent: Wednesday, June 30, 2010 12:20 PM
Subject: CEH Eligibility Application - request for exam code (Pearson Vue)

ALCON,

I am requesting an exam code to sit for your 312-33 Certified Ethical Hacking examination. Please find attached my exam application from your website, my passport photo for identification, and an official memo from my employer verifying that I exceed the experience requirements.

Thank you very much,

Ed Snowden

4 Attachments

UNCLASSIFIED

DEPARTMENT OF DEFENSE
SPECIAL REPRESENTATIVE JAPAN
UNIT #5100
APO AP 96328-5100
Officially Endorsed

By @Snare
I is for...

INTERNET

OF THINGS
Hacker 'shouts abuse' via Foscam baby monitoring camera

By Dave Lee
Technology reporter, BBC News

NB. Foscam is in no way related to Fosm
Fosm would NEVER shout at a baby. Not even for the LOLs
Japanese toilet users vulnerable to Bluetooth bidet assaults

By Aaron Souppouris (http://www.theverge.com/users/Aaron%20Souppouris) on August 3, 2013 04:52 pm

Email (mailto:aaron@theverge.com)

(http://twitter.com/intent/user?screen_name=AaronIsSocial)

ボタンをタッチして

say “gidday to the bidet”
J is for....

JUICE

JACKING
FREE CELL PHONE CHARGING KIOSK
YOU SHOULD NOT TRUST PUBLIC KIOSKS WITH YOUR SMART PHONE.

INFORMATION CAN BE RETRIEVED OR DOWNLOADED WITHOUT YOUR CONSENT. LUCKILY FOR YOU, THIS STATION HAS TAKEN THE ETHICAL ROUTE AND YOUR DATA IS SAFE.

ENJOY THE FREE CHARGE!
K is for....

KIOSK
Prisoners accessed internet through faulty computer kiosks - inquiry

By Adam Bennett Adam
12:39 PM Wednesday Jun 5, 2013

File photo / NZ Herald

Prisoners in privately run Mt Eden Corrections Facility were able to access the internet through faulty computer kiosks.
Prime Minister John Key says a major security flaw at Work and Income kiosks is a “huge problem,” and the Government has to work out what caused it.
L is for....

LEGAL ACTION
12 October 2011

Mr Patrick Webster

Dear Sir

Unauthorised access to member statements

We act for FSS Trustee Corporation (Trustee), the trustee of the First State Super scheme (Fund).

We refer to your email dated 22 September 2011 to Mr Adam Jarrett of Pillar, the Fund’s administrator, in which you described your unauthorised access to the statements of approximately 568 other members of the Fund.

Whilst you have indicated that your actions were motivated by an attempt to show that it is possible for a wrongdoer to obtain unauthorised access to Pillar’s systems, your actions may themselves be considered a breach of section 308H of the Crimes Act 1900 (NSW) and section 478.1 of the Criminal Code Act 1995 (Cth). You should be aware that due to the serious nature of your actions, this matter has been reported to the NSW Police.
Stunned MP weighs legal action

By Claire Trevett @CTrevettNZH Claire
5:30 AM Saturday Aug 3, 2013

Reporter's employer alleges cover-up after emails shown to have also been released

Peter Dunne is considering legal action after what he called a serious breach of privacy. Photo / Mark Mitchell

United Future leader Peter Dunne is considering legal action and Fairfax Media is alleging a "cover up" after it emerged yesterday that Mr Dunne's emails with reporter Andrea Vance were sent to an inquiry investigating the disclosure of a sensitive report.

The latest twist in the Henry Inquiry saga follows earlier revelations that Vance's phone records were sent to the inquiry, along with logs of her movements around the parliamentary precinct recorded by a swipecard.
M is for....

MALWARE

and also for METSERVICE

(who got mangled by Malware)
A file containing JavaScript code was uploaded into the MetService ad database, redirecting browsers to a malicious website.
N is for....
Rainbow Dragon
(Wrapped in asparagus cream cheese & mayonnaise)

Rainbow Roll
(Wrapped in assorted fish with tempura shrimp & tobiko & mayonnaise)

Red Monster
(California Roll, topped with an assortment of fish & caviar)

Faily Monster
(Spicy tuna top of mix kani, green onion)

Jumbo Shrimp Roll
(Wrapped in avocado ebi with jumbo shrimp, cucumber & mayonnaise)

Tuna Oyster Roll
(Wrapped in spicy tuna & egg)

GFE = Google Front End Server
SSL Added and removed here!
Traffic in clear text here.
O is for...

ONLINE AUCTIONS

and

OWASP TOP 10
Security mess sends Kiwi auction site titsup in two days

Holes allowed auction price resets, exposed passwords

By Simon Sharwood, 5 Oct 2012

A New Zealand auction website has shut after just a day, thanks to IT professionals who noticed extraordinarily relaxed security operations.

The site in question is Wheedle.co.nz, which currently says “unforeseen technical problems “have “postponed further activity on the website.”

Postp0wned may be a more accurate term, as blogger Ben Gracewood noticed the URL wheedle.co.nz/search/editprice. Visitors to that address could indeed edit the price of goods up for auction, and even peer at the reserve price. Other users complained of a password reset scheme that saw their secret words sent in plaintext in emails.

All allegations also surfaced that the software responsible for sending out password reminders had been accessed, with the result that account holders received multiple password-related emails.
P is for.... PKI
Maintenance

Due to a security breach that occurred on June 15th, issuance of digital certificates and related services has been suspended. Our services will remain offline until further notice.

Subscribers and holders of valid certificates are not affected in any form.

Visitors to websites and other parties relying on valid certificates are not affected.

We apologize for the temporary inconvenience and thank you for your understanding.
PKI Hall of Shame

* Comodo
* DigiNotor
* StartSSL
* Global Sign
* Apple
* Microsoft
Q is for....

QR CODES
Google Glass hacked by a simple QR code: New tech means new exploits
As we continue to empower more of our live with connected devices, the door is wide open for new attacks from hackers

Malicious QR Codes Pushing Android Malware

Denis
Kaspersky Lab Expert
Posted September 30, 14:43 GMT
Tags: Mobile Malware, Google Android

According to Wikipedia QR code is a type of matrix barcode (or two-dimensional code) first designed for the automotive industry. QR codes are becoming more and more popular today and are used in banners, magazines, transport and badges in order to provide quick and easy access to particular information. A QR code has a pretty big capacity (compared to a simple barcode) and is able to store 7089 numeric characters or 4296 alphanumeric characters; and it is more than enough to store text or URL.
China’s QR Code Bullet Train Tickets Spill Your Personal Info

July 15, 2011 | at 8:30 pm | by Steven Millward

QR codes can reveal name & ID / passport number
R is for RSA
Every time I look at my RSA SecureID token I see PROTECTED BY PATENTS and I think GOOD FUCKING THING SINCE IT'S NOT PROTECTED BY SECURITY

about 1 month ago from web
RSA's 'Denial' Concerning $10 Million From The NSA To Promote Broken Crypto Not Really A Denial At All

from the between-the-lines... dept

On Friday, a very big story broke on Reuters, saying that the NSA had paid RSA $10 million in order to promote Dual EC DRBG encryption as the default in its BSAFE product. It had been suspected for a few years, and more or less confirmed earlier this year, that the NSA had effectively taken over the standards process for this standard, allowing it to hide a weakness, making it significantly easier for the NSA to crack any encrypted content using it.
S is for SONY.
4/04/11 Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit
20/04/11 Sony PSN Offline
26/04/11 PSN Outage caused by Rebug Firmware
26/04/11 PlayStation Network (PSN) Hacked
27/04/11 Ars readers report credit card fraud, blame Sony
28/04/11 Sony PSN hack triggers lawsuit. Sony says SOE Customer Data Safe
2/05/11 Sony Online Entertainment (SOE) hacked. SOE Network Taken Offline
3/05/11 Sony Online Entertainment (SOE) issues breach notification letter
5/05/11 Sony Brings In Forensic Experts On Data Breaches
6/05/11 Sony Networks Lacked Firewall, Ran Obsolete Software: Testimony
7/05/11 Sony succumbs to another hack leaking 2,500 "old records"
14/05/11 Sony resuming PlayStation Network, Qriocity services
17/05/11 PSN Accounts still subject to a vulnerability
20/05/11 Phishing site found on a Sony server
21/05/11 Hack on Sony-owned ISP steals $1,220 in virtual cash
21/05/11 Sony Music Indonesia Defaced By k4L0ng666
22/05/11 Sony BMG Greece the latest hacked Sony site
23/05/11 LulzSec leak Sony's Japanese Websites
24/05/11 Sony says hacker stole 2,000 records from Canadian site (Sony Ericsson)
25/05/11 Sony Begins Providing ID Theft Protection for PlayStation Hack
2/06/11 LulzSec versus Sony Pictures
2/06/11 Sony BMG Belgium (sonybmg.be) database exposed
2/06/11 Sony BMG Netherlands (sonybmg.nl) database exposed
3/06/11 Sony Europe database leaked
5/06/11 Latest Hack Shows Sony Didn’t Plug Holes
5/06/11 Sony Pictures Russia (www.sonypictures.ru) dbs leaked
6/06/11 LulzSec Hackers Post Sony Computer Entertainment Developer Network
6/06/11 LulzSec hits Sony BMG, leaks internal network maps
8/06/11 Sony Portugal latest to fall to hackers
8/06/11 Spoofing lead to fraud via shopping coupons at Sonisutoa / My Sony Club (Google Translation)
11/06/11 Spain Arrests 3 Suspects in Sony Hacking Case
20/06/11 SQLI on sonypictures.fr
23/06/11 Class Action Lawsuit Filed Against Sony/SCEA
28/06/11 Sony CEO asked to step down on heels of hacking fiasco
6/07/11 Hackers posts fake celebrity stories on Sony site
12/10/11 Sony Press Release: 93,000 PSN Account Passwords Compromised
T is for....
TARGET
and
TRUSTWAVE
Target missed many warning signs leading to breach: U.S. Senate report

BY DOINA CHIACU

Target Breach Update:
1/3 US Adults At Risk

Target Corporation
NYSE: TGT - Mar 25 6:39 PM ET

59.06  -0.40 (-0.67%)  
After Hours: 59.06  0.00 (0.00%)

Open  59.59  
High  59.60  
Low   58.60  
Volume 0  
Avg Vol 7,064,000  
Mkt Cap 37.4B
WE'RE WATCHING YOU
Dear Faily,

You *could* tell them the truth Faily...

....but we would *strongly* suggest you don’t...

<3

Your friends at RSA/NSA
U is for...

UNEMPLOYED

TRUCKIE
Unemployed truck driver hacks NBN and controls it for six weeks. Now that is security!

by Pirate
Posted on 27-07-2011 10:21 AM

AN UNEMPLOYED truck driver with the online moniker "Evil" hacked into one of the national broadband network's service providers and had control of its entire system for at least six weeks, police allege.

In the first solo hacking case of its kind in Australia, federal police yesterday arrested the 25-year-old man at his home in the NSW central west town of Cowra.

He was expected to be charged with 50 offences over alleged incursions into Platform Networks, one of the first 12 service providers selected for the contentious $36 billion NBN trials.

Source
V is for...

VATICAN
Someone Inside The Vatican Is Pirating Video Games

LUKE PLUNKETT TODAY 3:00 AM

Last year’s version of divorce simulator Football Manager contained an interesting hidden secret: there was code inside that let the developers track the IP of everybody who pirated a copy of the game.

Speaking at the London Games Conference, attended by MCV, the results the developers disclosed are fascinating. Over 10 million copies were passed around illegally, with the naughtiest nations responsible being China, Turkey and Portugal.

Italy was also up there in the rankings though, and of the 547,000 copies Sega were able to trace to the country, one was from inside the Vatican.
W is for....

Wi-Fi
** Internet **

Network: PAGEANT
Password: beafce6161
PSC Wi-Fi Access

SSID: marko
swd: w3Lc0m3!HERE

NEW PASSWORD *****
and is case-sensitive
e to “Forget” or “Remove”
W is also for...
X is for....

X-RATED
'Sesame Street' YouTube channel back after porn hack

By Doug Gross, CNN
October 17, 2011 -- Updated 1706 GMT (0106 HKT) | Filed under: Web

Hackers commandeered the YouTube page of the "Sesame Street" children's show Sunday, adding pornographic videos.
AIM Investigates Alleged Database Compromise

XBIZ REPORT

By David Maxwell

Thursday, Mar 31, 2011  Text size: 📣 +1

LOS ANGELES — AIM Medical Associates is investigating various reports that say information from its database was compromised.

LA Times reported that the legal names, birthdates and stage names of more than 12,000 current and former adult performers were posted on Pornwikileaks.com, which is registered in the Netherlands, but it’s not clear who owns the site. Published reports suggest that the leaked information came from AIM Medical Associates.

XBIZ Research

What impact has mainstream social media had on the world of adult entertainment?
Y is for....

YIKES!!!!!!!
FOR NEARLY TWO DECADES THE NUCLEAR LAUNCH CODE AT ALL MINUTEMAN SILOS IN THE UNITED STATES WAS OOOOOOOOO

KARL SMALLWOOD  NOVEMBER 29, 2013  22
Z is for... 

ZEUS
Security Theatre brought to you by:
The letter F & the number 666
Today's teachers: FOBSKI & FOSM
Thanks to:

* Thomas Lim

* SYSCAN Organisers and Crew

* the kiwicön krüe

* the assembled h@x0rs
Contact us:

F is for Fail
@failymonster

Search for jobs

Jobs you may be interested in

Get email alerts
Your job activity is private.

HAYS
Recruiting experts worldwide

Deloitte.
New Zealand

Datacom

SAP SECURITY CONSULTANT
Auckland, New Zealand

SAP Security Consultant
Auckland, New Zealand

Information Architect - Web
Wellington