Slide of the Day – Security Matters

http://www.schneier.com/essay-028.html

Bruce Schneier

Security Pitfalls in Cryptography

by Bruce Schneier
1998

You can download this essay in PDF (Acrobat) format or as a PalmPilot DOC.

This essay is also available in a French translation.

Magazine articles like to describe cryptography products in terms of algorithms and key length. Algorithms make good sound bites: they can be explained in a few words and they're easy to compare with one another. "128-bit keys mean good security." "Triple-DES means good security." "40-bit keys mean weak security." "2048-bit RSA is better than 1024-bit RSA."

But reality isn't that simple. Longer keys don't always mean more security. Compare the cryptographic algorithm to the lock on your front door. Most door locks have four metal pins, each of which can be in one of ten positions. A key sets the pins in a particular configuration. If the key aligns them all correctly, then the lock opens. So there are only 10,000 possible keys, and a burglar willing to try all 10,000 is guaranteed to break into your house. But an improved lock with ten pins, making 10 billion possible keys, probably won't make your house more secure. Burglars don't try every possible key (a brute-force attack); most aren't even clever enough to pick the lock (a cryptographic attack against the algorithm). They smash windows, kick in doors, disguise themselves as policemen, or rob keyholders at gunpoint. One ring of art thieves in California defeated home security systems by taking a chainsaw to the house walls. Better locks don't help against these attacks.

Strong cryptography is very powerful when it is done right, but it is not a panacea. Focusing on the cryptographic algorithms while ignoring other aspects of security is like defending your house not by building a fence around it, but by putting an immense stake into the ground and hoping that the adversary runs right into it. Smart attackers will just go around the algorithms.

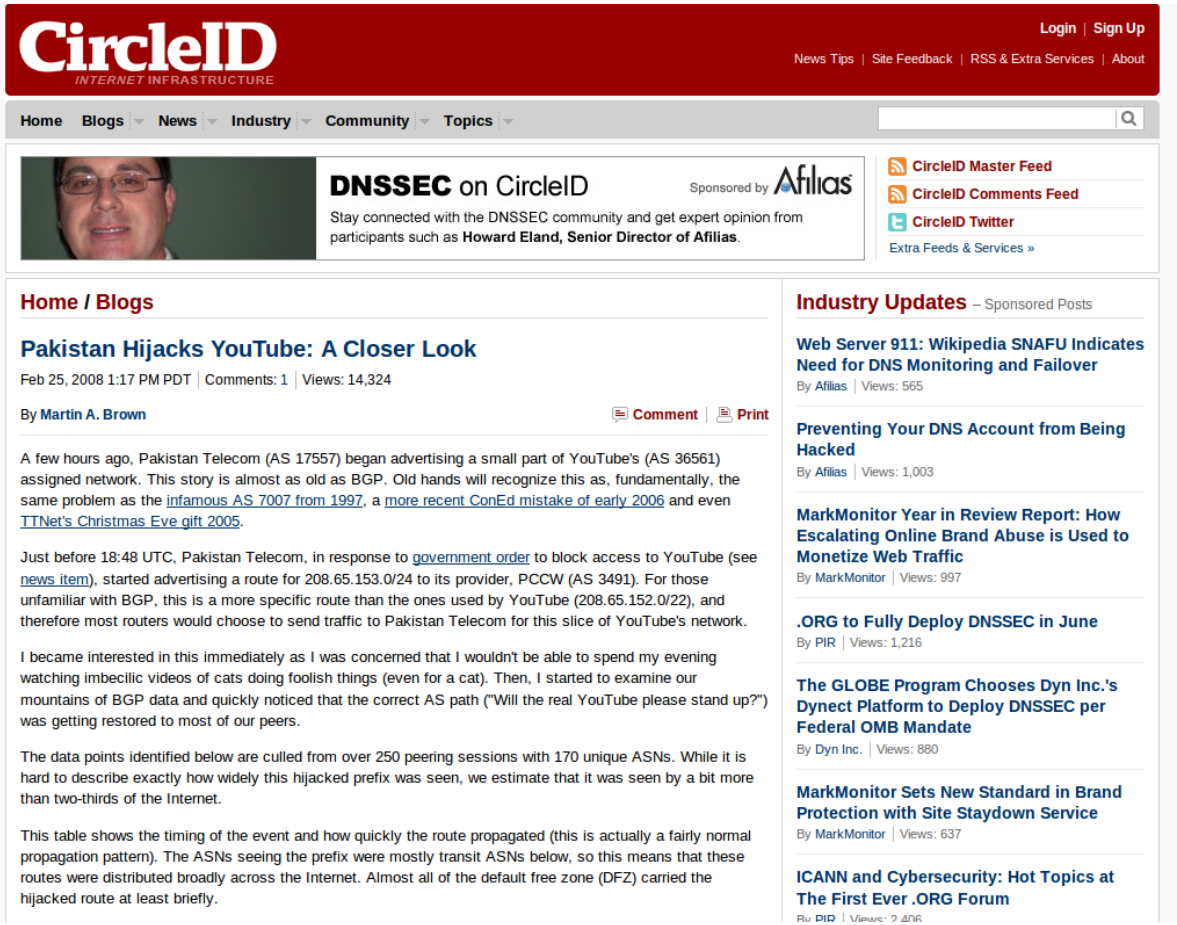
Counterpane has spent years designing, analyzing, and breaking cryptographic systems. While we do research on published algorithms and protocols, most of our work examines actual products. We've designed and analyzed systems that protect privacy, ensure confidentiality, provide fairness, and facilitate commerce. We've worked with software, stand-alone hardware, and everything in between. We've broken our share of algorithms, but we can almost always find attacks that bypass the algorithms altogether. We don't have to try every possible key, or even find flaws in the algorithms. We exploit errors in design, errors in implementation, and errors in installation. Sometimes we invent a new trick to break a system, but most of the time we exploit the same old mistakes that designers make over and over again.

Attacks Against Cryptographic Designs

A cryptographic system can only be as strong as the encryption algorithms, digital signature algorithms, one-way hash functions, and message authentication codes it relies on. Break any of them, and you've broken the system. And just as it's possible to build a weak structure using strong materials, it's possible to build a weak cryptographic system using strong algorithms and protocols.

Slide of the Day – Security Matters

http://www.circleid.com/posts/82258_pakistan_hijacks_youtube_closer_look



CircleID
INTERNET INFRASTRUCTURE

Login | Sign Up
News Tips | Site Feedback | RSS & Extra Services | About

Home | Blogs | News | Industry | Community | Topics

DNSSEC on CircleID
Sponsored by Afilias
Stay connected with the DNSSEC community and get expert opinion from participants such as **Howard Eland, Senior Director of Afilias**.

CircleID Master Feed
CircleID Comments Feed
CircleID Twitter
Extra Feeds & Services »

Home / Blogs

Pakistan Hijacks YouTube: A Closer Look

Feb 25, 2008 1:17 PM PDT | Comments: 1 | Views: 14,324

By Martin A. Brown

Comment | Print

A few hours ago, Pakistan Telecom (AS 17557) began advertising a small part of YouTube's (AS 36561) assigned network. This story is almost as old as BGP. Old hands will recognize this as, fundamentally, the same problem as the infamous AS 7007 from 1997, a more recent ConEd mistake of early 2006 and even TTNet's Christmas Eve gift 2005.

Just before 18:48 UTC, Pakistan Telecom, in response to government order to block access to YouTube (see news item), started advertising a route for 208.65.153.0/24 to its provider, PCCW (AS 3491). For those unfamiliar with BGP, this is a more specific route than the ones used by YouTube (208.65.152.0/22), and therefore most routers would choose to send traffic to Pakistan Telecom for this slice of YouTube's network.

I became interested in this immediately as I was concerned that I wouldn't be able to spend my evening watching imbecilic videos of cats doing foolish things (even for a cat). Then, I started to examine our mountains of BGP data and quickly noticed that the correct AS path ("Will the real YouTube please stand up?") was getting restored to most of our peers.

The data points identified below are culled from over 250 peering sessions with 170 unique ASNs. While it is hard to describe exactly how widely this hijacked prefix was seen, we estimate that it was seen by a bit more than two-thirds of the Internet.

This table shows the timing of the event and how quickly the route propagated (this is actually a fairly normal propagation pattern). The ASNs seeing the prefix were mostly transit ASNs below, so this means that these routes were distributed broadly across the Internet. Almost all of the default free zone (DFZ) carried the hijacked route at least briefly.

Industry Updates – Sponsored Posts

Web Server 911: Wikipedia SNAFU Indicates Need for DNS Monitoring and Failover
By Afilias | Views: 565

Preventing Your DNS Account from Being Hacked
By Afilias | Views: 1,003

MarkMonitor Year in Review Report: How Escalating Online Brand Abuse is Used to Monetize Web Traffic
By MarkMonitor | Views: 997

.ORG to Fully Deploy DNSSEC in June
By PIR | Views: 1,216

The GLOBE Program Chooses Dyn Inc.'s Dynect Platform to Deploy DNSSEC per Federal OMB Mandate
By Dyn Inc. | Views: 880

MarkMonitor Sets New Standard in Brand Protection with Site Staydown Service
By MarkMonitor | Views: 637

ICANN and Cybersecurity: Hot Topics at The First Ever .ORG Forum
By PIR | Views: 2,406

Slide of the Day – Security Matters

- http://www.heise.de/security/meldung/Chinesischer-Provider-entfuehrt-kurzzeitig-Teile-des-Internets-975137.html

heise Security

Security › News › 2010 › KW 15 › Chinesischer Provider "entführt" kurzzeitig Teile des Inte

Sie sind Gast
Einloggen | Registrieren

Suche
los!
Im Browser einrichten

News
7-Tage-Alerts
7-Tage-News
News-Archiv
Newsletter
English News
News mobil
RSS-Feed

Anzeige
SICHERHEIT IN EINER VERTEILTEN WELT
HEISE SECURITY TOUR 2010

Hintergrund

News-Meldung vom 12.04.2010 11:25 « Vorige | Nächste »

Chinesischer Provider "entführt" kurzzeitig Teile des Internets

vorlesen / MP3-Download

Der kleinere chinesische Internet-Provider IDC China hat sich Berichten zufolge durch einen Konfigurationsfehler eines BGP-Routers kurzzeitig für das Routing zu rund 37.000 IP-Netzen zuständig erklärt. Über das Border-Gateway-Protocol signalisieren sich Router, für welche Netze (autonome Systeme, AS) sie zuständig sind und welche anderen Netze sie erreichen können.

Anzeige
IBM
IBM System x Announcement
Smarter systems for a Smarter Planet:
Erfahren Sie mehr
heise online

Hauptsächlich soll der chinesische Provider Routen zu Netzen (BGP Prefixes) verkündet haben, die zu anderen Providern in den USA und China gehören. Zu den propagierten Netzen sollen auch die von Dell, CNN, Apple, www.amazon.de,

Slide of the Day – Security Matters

- http://www.heise.de/security/meldung/Cross-Site-Scripting-mit-Meta-Informationen-972908.html

heise Security

Sie sind Gast
Einloggen | Registrieren

Suche
los!
Im Browser einrichten

News
7-Tage-Alerts
7-Tage-News
News-Archiv
Newsletter
English News
News mobil
RSS-Feed

Anzeige

Security › News › 2010 › KW 14 › Cross-Site-Scripting mit Meta-Informationen

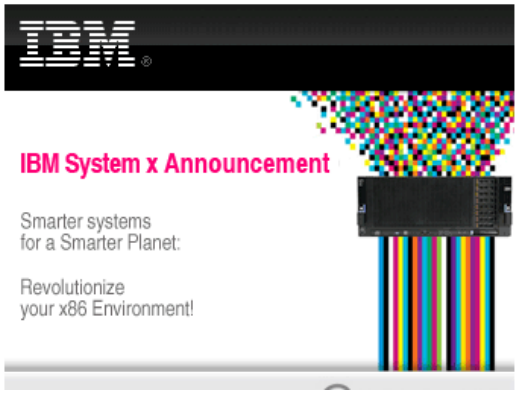
News-Meldung vom 08.04.2010 13:39 « Vorige | Nächste »

Cross-Site-Scripting mit Meta-Informationen

vorlesen / MP3-Download

Datenfelder zur Aufnahme von Meta-Informationen bieten einen weiten Spielraum für kommende Cross-Site-Scripting-Angriffe (XSS), behauptet der Sicherheitsspezialist Tyler Reguly von nCircle. So lässt sich etwa in Whois- und DNS-Datensätzen sowie in SSL-Zertifikaten eingebettetes JavaScript unter bestimmten Umständen im Browser ausführen. Beispielsweise gibt es Web-Dienste, die eine Online-Prüfung von SSL-Zertifikaten von anderen Servern durchführen können. Unter anderem zeigen solche Dienste neben kryptografisch relevanten Informationen auch die Daten zum Inhaber und Aussteller des Zertifikats an.

Anzeige



Slide of the Day – Security Matters

http://www.wired.com/politics/security/news/2009/04/fleetcom?currentPage=all

POLITICS : SECURITY

The Great Brazilian Sat-Hack Crackdown

By Marcelo Soares 04.20.09

Brazilian satellite hackers use high-performance antennas and homebrew gear to turn U.S. Navy satellites into their personal CB radios.
Photo: Divulgação/Policia Federal

Slide of the Day – Security Matters

http://news.cnet.com/8301-1009_3-10417247-83.html

home | reviews | news | downloads | cnet tv On last.fm: Hip-hop radio - Listen free!

cnet news

Latest News | CNET River (BETA) | Webware | Crave | Business Tech | Green T

Home > News > Security

Security

December 17, 2009 6:48 AM PST

Predator drones hacked in Iraq operations

by Declan McCullagh Font size Print E-mail Share 74 comments

142 retweet Share 144

Iraqi insurgents have reportedly intercepted live video feeds from the U.S. military's **Predator drones** using a $25.95 Windows application that allows them to track the pilotless aircraft undetected.

Hackers working with Iraqi militants were able to determine which areas of the country were under surveillance by the U.S. military, **The Wall Street Journal reported** Thursday, adding that video feeds from drones in Afghanistan also appear to have been compromised.

Meanwhile, a senior Air Force officer said Wednesday that a wave of new surveillance aircraft, both manned and unmanned, were being deployed to Afghanistan to **bolster "eyes in the sky" protection** for the influx of American troops ordered by President Obama.

The MQ-1 Predator.
(Credit: U.S. Air Force)

This apparent security breach, which had been known in military and intelligence circles to be possible, arose because the Predator unmanned aerial vehicles do not use encryption in the final link to their operators on the ground.

Read more of "**U.S. was Warned of Predator Drone Hacking**" at CBSNews.com.

Slide of the Day – Security Matters

http://tech.slashdot.org/article.pl?sid=09/04/09/2044205

Slashdot NEWS FOR NERDS. STUFF THAT MATTERS.

Log In Create Account Help Subscribe Firehose

▼ Slashdot
Apple
Ask Slashdot
Book Reviews
Games
Hardware
Idle
Interviews
Linux
Mobile
Science
Technology
YRO
▼ Site Info
FAQ
Bugs
Code
▼ Stories
Old Stories

Multiple Fiber Cuts In San Francisco Area

Posted by timothy on Thu Apr 09, 2009 04:55 PM
from the shame-if-anything-bad-was-to-happen dept.

georgewilliamherbert writes

> "Multiple news reports, mailing list posts, blogs, and tweets are pointing out two overnight acts of sabotage in the San Francisco Bay area, with long distance fiber network cables being cut in two locations in the early morning hours. The first cut, around 1:30 AM, affecting landline and cell phone service and 911 calls in the communities of Morgan Hill, Gilroy, and parts of Santa Cruz counties, was on an AT&T fiber alongside Monterey Highway near Blossom Hill Road, in San Jose. A second cut, around 3:30 AM, in San Carlos, affected Sprint fiber and has significantly disrupted services at the 200 Paul datacenter in southern San Francisco. Rumor says that this may be related to a AT&T communications workers contract having just expired — but no evidence has been published yet in the media, and this could be an intentional act of sabotage by someone unrelated to the company's workers."

▶ internet networking story

Related Stories

Submission: Multiple fiber cuts in San Francisco area by georgewilliamherbert (211790)

Slide of the Day – Security Matters

http://www.barracudacentral.org/data/spam

Barracuda Networks | Barracuda Central | Barracuda Labs | BarracudaWare | phion | CudaTel | CudaEye

BARRACUDACENTRAL.org — Technical Insight for Security Pros

- Home
- About
- Contact
- **Spam Data**
- Web Data
- Virus Data
- BRBL
  - About
  - Request Access
  - Log In
  - Listing Methodology
  - Removal Request
  - How to Use
- Lookups
- Feedback
- Report Issues
- Additional Resources
- EmailReg.org
- Barracuda Networks

Spam Data

Email Processed (last 2 days)

	Yesterday 04/14		Today 04/15 (so far)	
Blocked: Spam	1,807,938,384	90.41%	964,357,500	92.17%
Blocked: Virus	2,130,975	0.11%	646,700	0.06%
Quarantined	9,730,052	0.49%	4,911,343	0.47%
Allowed: Tagged	8,745,753	0.44%	4,004,503	0.38%
Allowed	171,142,458	8.56%	72,344,938	6.91%
Total Received	1,999,687,622	100.00%	1,046,264,984	100.00%

Last Updated Last Updated 04/15/10 15:30:40 GMT

Hourly Email Activity over last 24 Hours

Top Spam Sources by Country

Country	% of Total Spam	Country	% of Total Spam
1 - United States	23.58%	6 - Netherlands	3.77%
2 - Brazil	6.77%	7 - Germany	3.52%
3 - Russia	5.66%	8 - China	3.38%
4 - Canada	4.69%	9 - United Kingdom	2.48%
5 - Turkey	4.24%	10 - Poland	2.25%

Top Spam Categories

Slide of the Day – Security Matters

http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

Steve Friedl
UNIXWIZ.NET

- Home
- Contact
- About
- TechTips
- Tools&Source
- Evo Payroll
- Research
- AT&T 3B2
- Advisories
- News/Pubs
- Literacy
- Calif.Voting
- Personal
- Tech Blog
- SmokeBlog

Steve Friedl's Unixwiz.net Tech Tips

An Illustrated Guide to the Kaminsky DNS Vulnerability

The big security news of Summer 2008 has been Dan Kaminsky's discovery of a serious vulnerability in DNS. This vulnerability could allow an attacker to redirect network clients to alternate servers of his own choosing, presumably for ill ends.

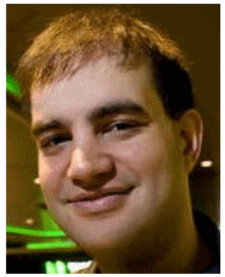
Table of Contents

This all led to a mad dash to patch DNS servers worldwide, and though there have been many writeups of just how the vulnerability manifests itself, we felt the need for one in far more detail. Hence, one of our Illustrated Guides.

This paper covers how DNS works: first at a high level, then by picking apart an individual packet exchange field by field. Next, we'll use this knowledge to see how weaknesses in common implementations can lead to cache poisoning.

By fully understanding the issues at play, the reader may be better equipped to mitigate the risks in his or her own environment.

We hope everybody who runs a DNS server patches soon.



Nice work, Dan

Terminology

Slide of the Day – Security Matters

http://www.wired.com/threatlevel/2010/03/packet-forensics/

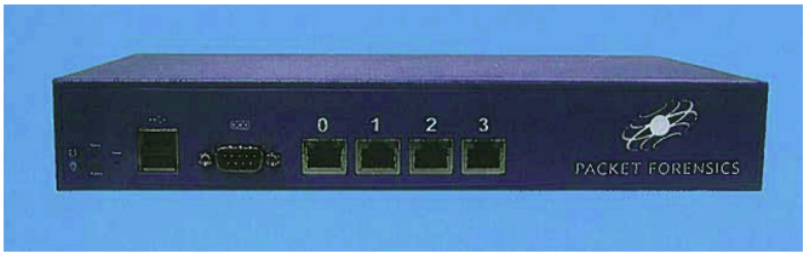
WIRED SUBSCRIBE » SECTIONS » BLOGS » REVIEWS » VIDEO » HOW-TOS »
Sign In | RSS Feeds

THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

Law Enforcement Appliance Subverts SSL

By Ryan Singel | March 24, 2010 | 1:55 pm | Categories: Surveillance, Threats



That little lock on your browser window indicating you are communicating securely with your bank or e-mail account may not always mean what you think its means.

Normally when a user visits a secure website, such as Bank of America, Gmail, PayPal or eBay, the browser examines the website's certificate to verify its authenticity.

At a recent wiretapping convention, however, security researcher Chris Soghoian discovered that a small company was marketing internet spying boxes to the feds. The boxes were designed to intercept those communications — without breaking the encryption — by using forged security certificates, instead of the real ones that websites use to verify secure connections. To use the appliance, the government would need to acquire a forged certificate from any one of more than 100 trusted Certificate Authorities

Slide of the Day – Security Matters

- http://www.zdnet.co.uk/news/security-threats/2010/02/11/chip-and-pin-is-broken-say-researchers-40022674/2/

ZDNet

Search

UK Edition | News | Reviews | Blogs | Apple | Broadband | Cloud | DigitalGov | Google

ZDNet UK / News and Analysis / Security / Security Threats

Chip and PIN is broken, say researchers

By Tom Espiner, ZDNet UK, 11 February, 2010 17:01

Topics

Chip and PIN, Hack, Credit card, Debit card, Man in the middle, EMV protocol, Cambridge University, UK Payments Administration, Scam, Fraud, PIN

Sponsored Links

Loxit Laptop Trolleys
for 8-32 Laptops, All sizes. High Security, Welded Steel & Safe Locks
www.loxit.com

Virtual Backup Software
Use virtual infrastructure to back up. esXpress™4.0 30 day free trial
www.phdvirtual.com

Sicherheitsberatung
Informationssicherheit-

...that it stores on its chip. If the PIN is correct, the card sends a verification code — 0x9000 — back to the terminal, which completes the transaction.

The researchers succeeded in building a man-in-the-middle device that reads a card and — at the appropriate time in the verification process — sends a 0x9000 code to the terminal, regardless of the PIN that has been entered.

As a demonstration, the researchers inserted a genuine card into a standard smartcard reader from Alcor Micro, which was connected to a laptop running a Python script. The laptop was connected to an FPGA board via a serial link. The FPGA board the researchers used was a Spartan-3E Starter Kit, which was used to convert the interfaces for the card and PC.

The FPGA board was connected to a Maxim 1740 interface chip, which was linked via thin wires to a fake card, used for insertion in the terminal.

Once the fake card was inserted, the Python script running on the laptop relayed the transaction, suppressed the verify PIN command issued by the terminal, and responded with the 0x9000 code.

The researchers said that attackers could carry similar kit in a backpack, with the wires trailing down a sleeve, for use with a stolen valid card.

Consumer liability

Anderson noted that in disputed transactions, if the transaction has been verified by PIN, the liability for the loss rests on the consumer rather than on the bank or merchant.