THE MORE IT CHANGES, THE MORE IT STAYS THE SAME

RANDY MARCHANY
VA TECH IT SECURITY OFFICE

(C) MARCHANY 2011

WHO AM I?

CISO at VA Tech

- 35+K node network. dual stack IPV4, IPV6 network since 2006
- Multi-national – Main campus (Blacksburg, VA), Remote campuses (Arlington, Norfolk, VA), Swiss, Indian, Egyptian campuses

My IT Security Philosophy

All Security is Local

The Business Process trumps the Security Process

Learn the business process before imposing security requirements

Restrictive security practices cause worse problems overall

With SANS Institute since 1992

I'm instructor #2

The Register - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

9 November 2001
Updated: 15:02 GMT

The Register

Biting the hand that feeds IT

Search The Register

Go!

Sections

- Front Page
- Software
- Enterprise Systems
- Personal Hardware
- Semiconductors
- Internet
- Net Security
- Anti-Virus News
- Business
- Networks
- Bootnotes
- The Week's Headlines

Register Marketplace Buying?

Register Marketplace Selling?

- Assault on America
- Broadband
- e-business

Advertisement

ONLY £20 +VAT

Hacker jailed for revenge sewage attacks

By Tony Smith

Posted: 31/10/2001 at 15:55 GMT

Advertisement

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

"Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant of the Australian Environmental Protection Agency.

The Maroochydore District Court heard that

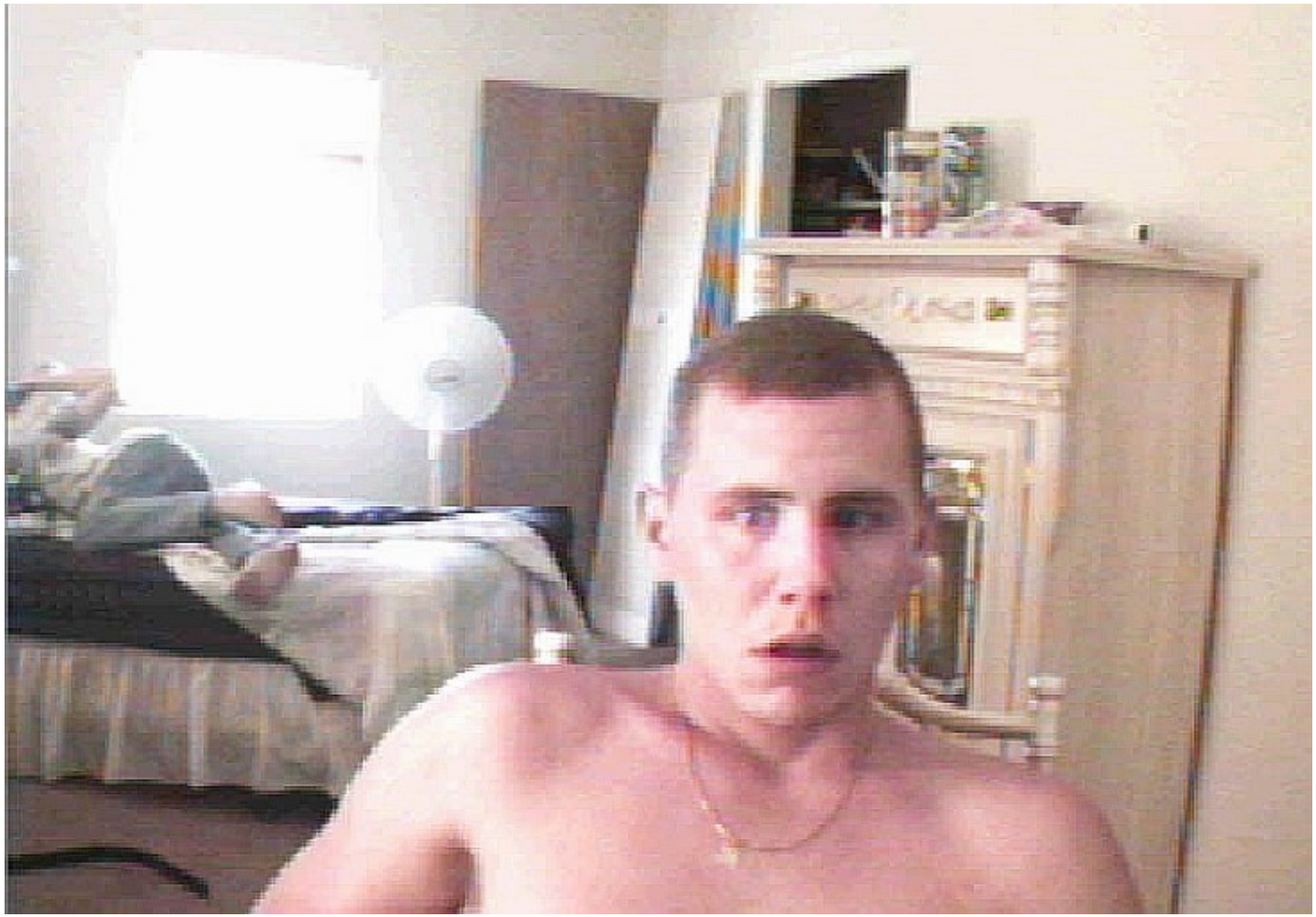
Advertisement

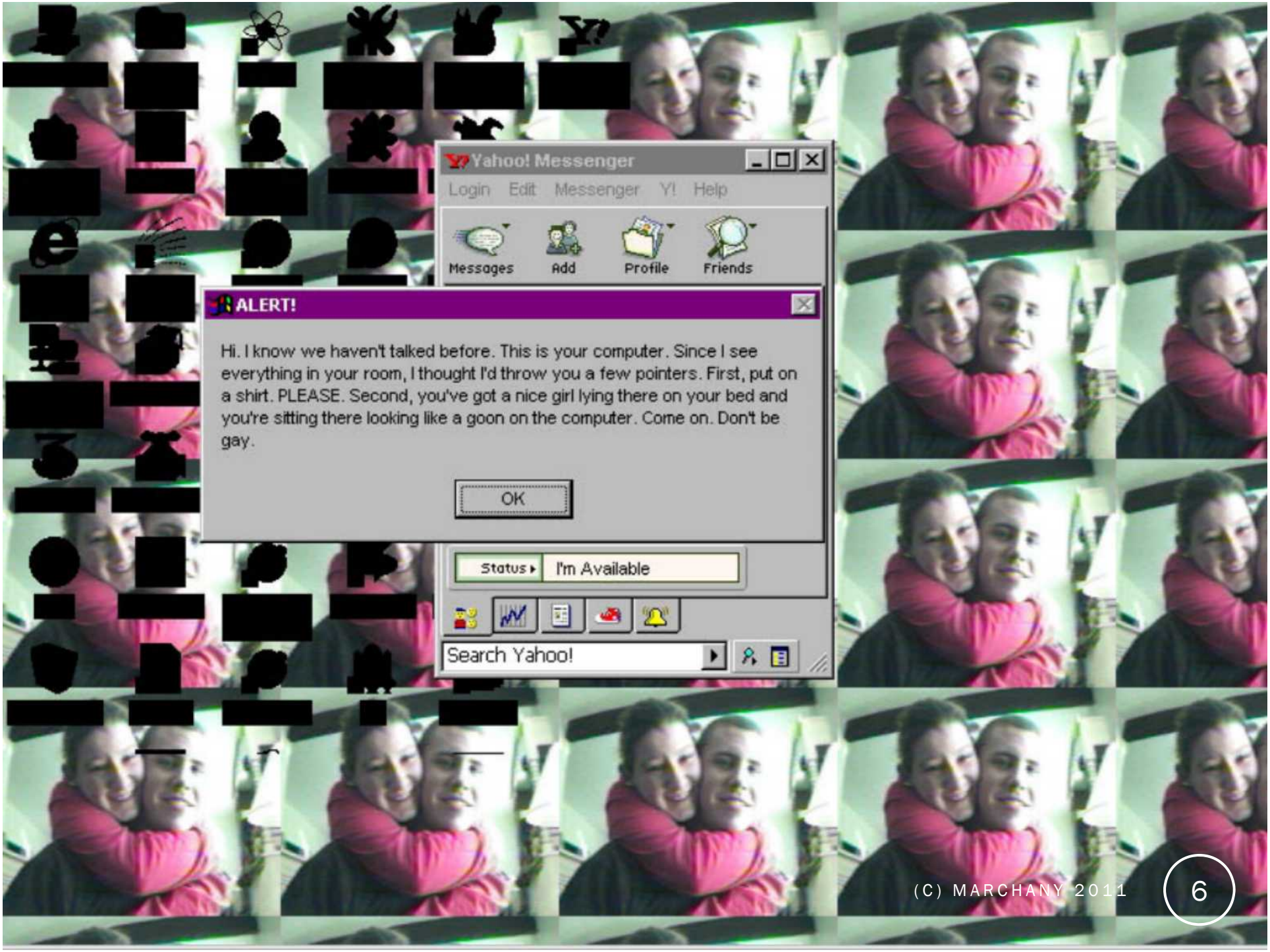
e-business Expo 27-29 november

7% of 9K

Start The Register - N... untitled - Paint 1:29 PM

STOP





(C) MARCHANY 2011

Partly sunny and warm
Highs: 70°-75°
Lows: 45°-50°

TOMORROW
Chance of showers
Highs: 65°-70°
Lows: 35°-40°

COLLEGIATE TIMES

97th Year, No. 44 ▪ Blacksburg, Virginia ▪ Friday, November 3, 2000

An independent student-run newspaper serving the Virginia Tech community since 1903

Tech computer used in Yankees hacking

by **Brian McNeill**
News Editor

A Virginia Tech computer was used in the hacking of the New York Yankees' website during the World Series last week, authorities said.

"A machine in the electrical engineering department was compromised by someone and was used in the Yankees hack," said Randy Marchany, a computer systems engineer and member of the computer incident response team, which handles online security for the university.

The hackers changed the Yankees.com numerical web address so online traffic would

the electrical engineering department, Marchany said.

Surfers expecting to see the Yankees' website were then greeted with pornographic pictures and the message "Yankees suck."

The FBI's New York office is looking into the crime.

"We are still investigating the hack of the Yankees' website," said Jim Margolin, special agent of the New York office of the FBI.

However, specific details of the investigation could not be disclosed until more developments unfold in the case, Margolin said.

"Since the investigation is ongoing, I can't say whether we have any strong leads or if there are any suspects," he said.

Marchany said he expects the hackers will most likely be caught in the near future.

"The FBI has a lot of evidence and we have a lot of evidence," he said. "We were very fast in containing the problem once we were notified of it."

Yankees.com notified Tech of the hack after their online security determined the connection to the electrical engineering computer, Marchany said.

The hackers do not necessarily have any connection to Tech, Marchany said, because the attack could have been perpetrated from anywhere. Hackers search the entire Internet to locate computer weaknesses they can exploit, he said.

"I think there are people that regularly scan the entire Internet for vulnerable machines," he said. "It's almost as if you were to try to open the door to every home in Blacksburg, document the results and go back later and break in."

Tech has had its share of computer attacks over the years, but the computer incident response team has always quickly solved the situations, Marchany said.

"In the past 10 years, there have been probably five major attacks," he said. "We've been very good about isolating and correcting the problems."

Address http://www.sans.org/newlook/home.htm Go Links

Fluffi Bunni ownz you.

A BamBam here a dotslash there
here a dot there a slash
everywhere a dot slash

look mommy im on sans !

Done Internet

WHAT I SAID: 1990'S – 2000'S

"Viruses, trojans and worms will never be eliminated. There is a multi-billion $ industry built to contain them." - RCM 2002

There's no economic incentive to eliminate the root causes of cybersecurity issues.

THE WORLD TODAY (2002)

A tremendous amount of personal information is on the web.

Personal data protection is hampered by

- Poorly designed vendor software
- Lack of user, data custodian awareness

BEWARE THE SOFTWARE LICENSE (2004)

Vendor license agreements do not favor the consumer. Duh!

EULA may be the popular solution for vendors to avoid being held responsible for security problems with their code.

Examples: KaZaA license agreement; limitations of liability

MOST COMMON SECURITY MISTAKES MADE BY INDIVIDUALS (2001)

Poor password management

Leaving your computer on, unattended

Opening e-mail attachments from strangers

Not installing anti-virus software

Laptops on the loose

Blabber mounts

Plug and Play without protection

Not reporting security violations

Always behind the times (OS, application patches)

Keeping an eye out inside the organization

13 THREATS TO VT (1996)

- No System Administrator Training
- PC, Mac Access control
- Bad Operational Policies
- Key Person Dependency
- Bad Passwords
- Internal Physical Security
- External Physical Security
- Cleartext data transmission
- Data disclosure of confidential information
- Forgery (spoofing) of data or email
- Large Scale disaster - fire
- Construction Mistakes

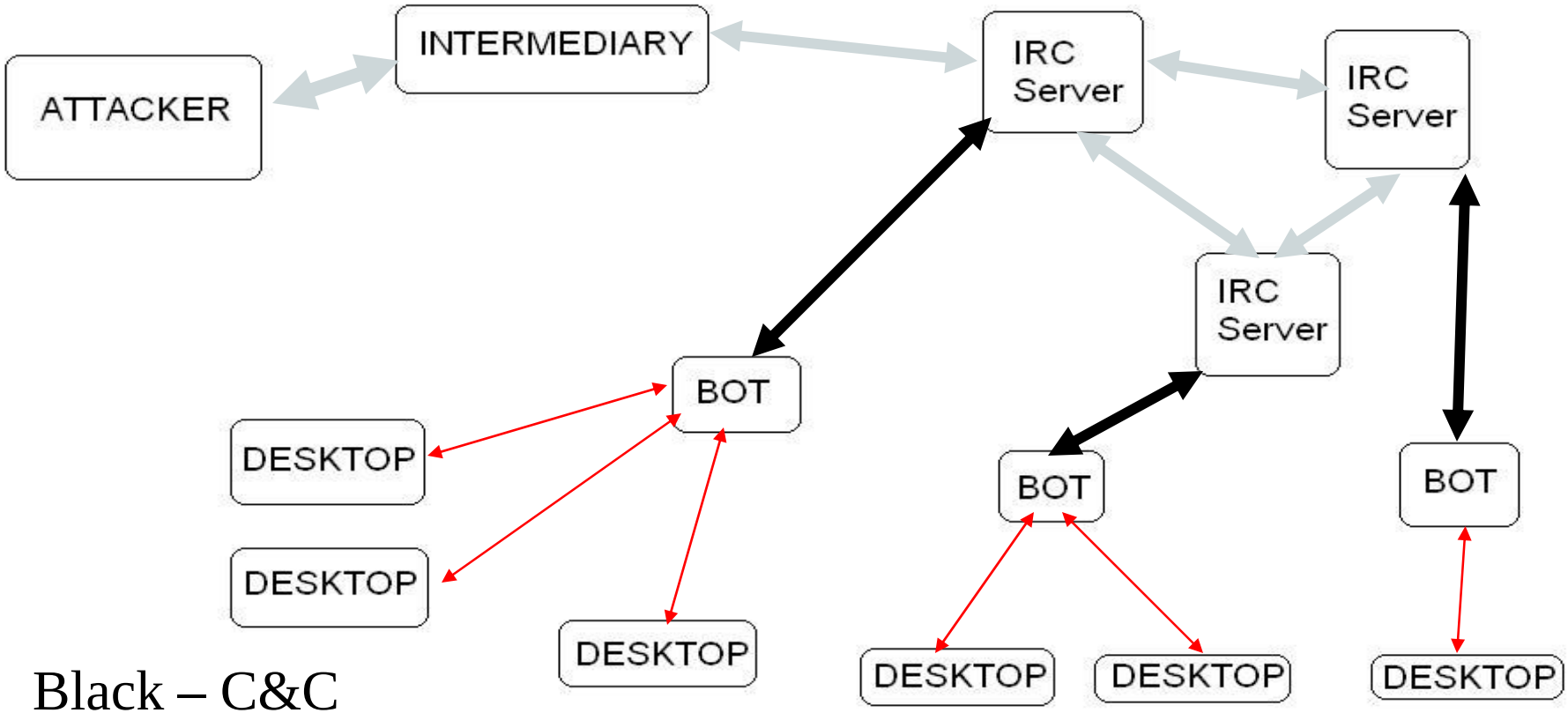
CLOUD COMPUTING – THE NEW THING!

Cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down providing for an on-demand utility-like model of allocations and consumption (2011)

The Network is the Computer (Sun Microsystems, 1997)

DDOS (1990S) -> BOTNET (2000S)

BOTNET (20xx) DDOS – 1990s



Black – C&C
Red – Scan info

WHY AREN'T WE FIXING THE REAL PROBLEM?

ENTIT

PECIAL REPORTS | EVENTS | EBOOKS | WHITEPAPERS | WEBINARS

for Free: Enter email | Sign up | About | View Sample | Privacy

Small coding mistake led to big Internet voting system failure

February 22, 2012 — 7:36am ET | By David Perera

TOOLS
- Subscribe
- Email
- Print
- Contact Author
- Reprint

TAGS
University Of Michigan
cybersecurity
electronic democracy
internet voting
voting systems
J. Alex Halderman

Image: State Dept.

The main security weakness that let University of Michigan researchers take control over a planned city of Washington, D.C. Internet voting system pilot for overseas voters in 2010 was "a tiny oversight in a single line of code," the researchers say in a new paper (.pdf) detailing their exploits. City officials canceled the pilot shortly before the November election after the hack was revealed.

It's evidence, say the researchers--led by Assistant Professor J. Alex Halderman--that Internet voting should be postponed until, when or if

SEARCH:

MOST POPULAR STORIES

Most Read | Most Emaile

- New DHS office tackles broadba steps
- DoD pushes for 'routine' UAV flig
- Papp addresses Coast Guard ar uncertainty for NSC program
- Small coding mistake led to big failure
- Being buddies still pays off in fe
- Terrorism a social activity, says

EVENTS

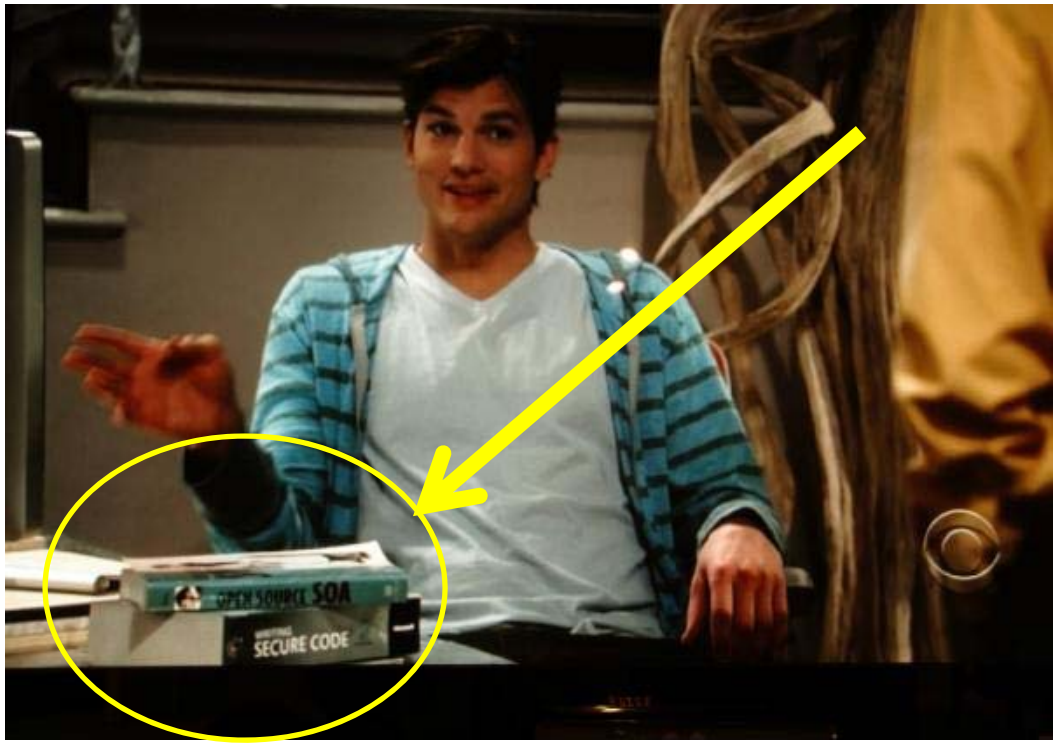
Learn With Your Peers at the Management Conference
April 15-18 — Cambridge, MD

V2X for Auto Safety and Mobi
March 20-21, 2012 — Novi, MI

TECHEXPO Top Secret Career
February 29, 2012 — Colorado S
3pm

More Events >>

:CT>:0



WE HAVE MET THE ENEMY & IT IS US

Major software vendor converts passwords to UPPER CASE, weak hashing of passwords

Major sites store passwords in the CLEAR!

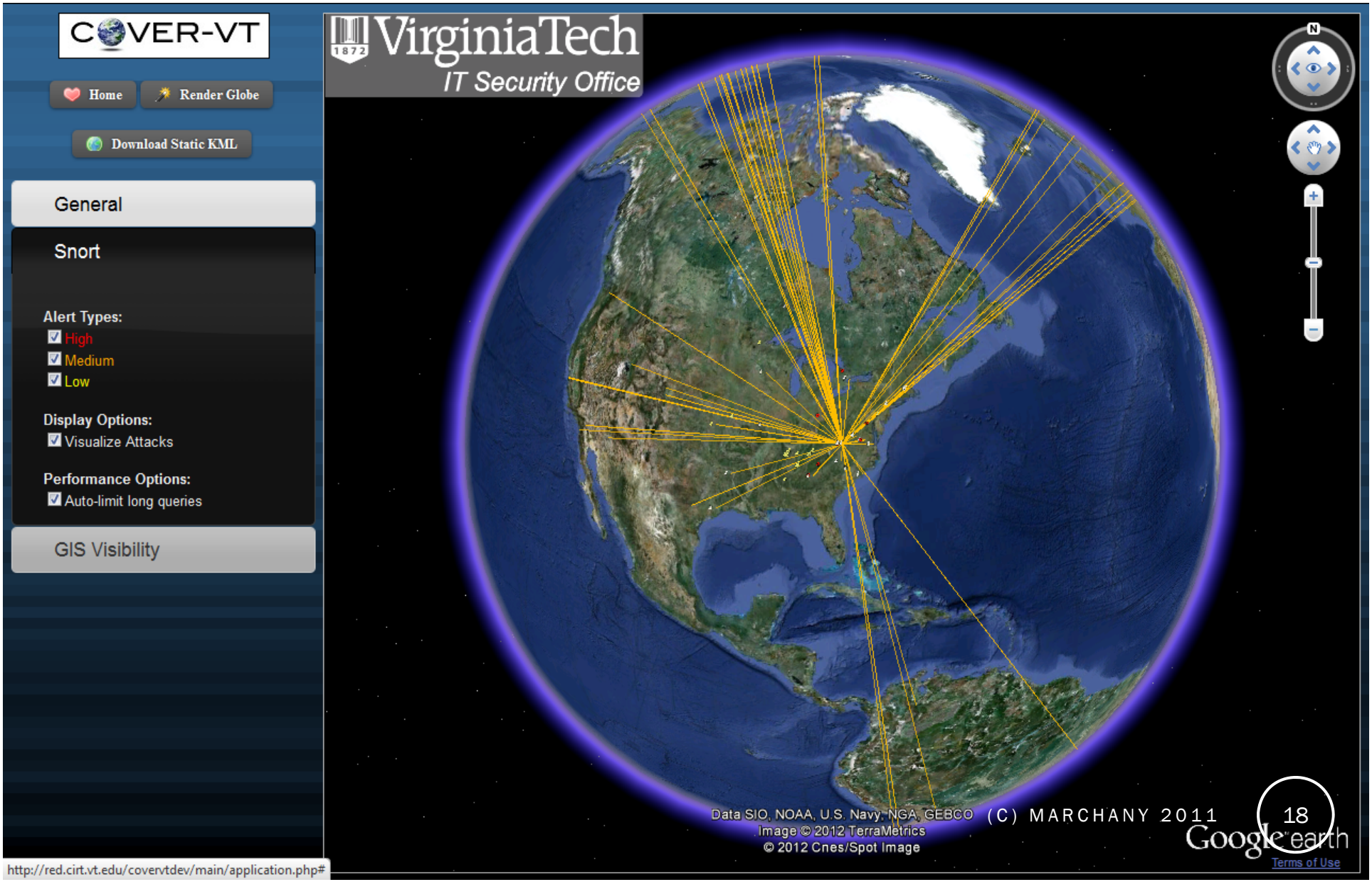
http://www.plaintextoffenders.com

WWW application software with SQL Injection, XSS vulnerabilities

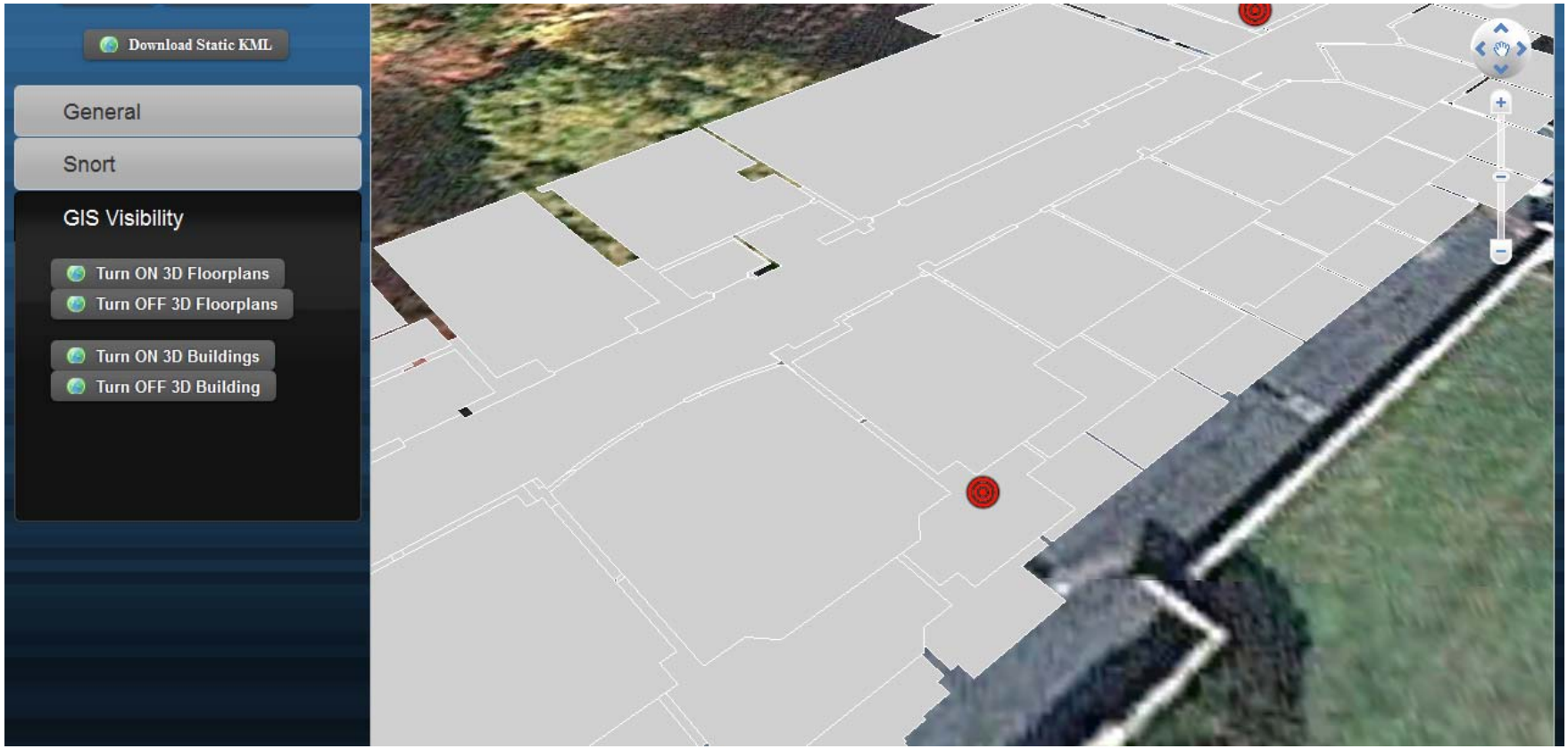
Some want to use your authentication systems

Why are we still buying these products?

CONVERGED SECURITY



TRACKING INSIDE A BUILDING



MISSION CONTROL, BUILT FOR CITIES

"..metropolitan areas already use data-collection systems like sensors, video cameras and GPS devices. But advances in computing power and data analysis now make it possible for companies like I.B.M. to collate all this data and, using computer algorithms, to identify patterns and trends.

http://www.nytimes.com/2012/03/04/business/ibm-takes-smarter-cities-concept-to-rio-de-janeiro.html?pagewanted=all

IS AUTOMATED RESPONSE THE WAY?

NYMAG.COM | THE MAGAZINE | DAILY INTEL | VULTURE | THE CUT | GRUB STREET LOG IN | REGISTER Like 76k Follow

Search GO

New York NEWS & FEATURES

HOME | NEWS & FEATURES | RESTAURANTS | BARS | ENTERTAINMENT | FASHION | SHOPPING | Agenda

PLUS TRAVEL | REAL ESTATE | VISITOR'S GUIDE | BEAUTY | DESIGN | WEDDINGS | BEST DOCTORS | DATING | BEST OF NY New York: Subscribe Today | Give a Gift

« Alligator Bites Off Florida Man's Hand; He's Charged for Feeding It

DAILY Intel

CNN Accidentally Plays Pink's 'Stupid Girls' Before Segment About Palin and Chick-fil-A »

7/30/12 at 12:25 AM | Comment

NYPD to Launch 'All-Seeing' 'Domain Awareness System'

By Brett Smiley

Watching you.

Police Commissioner Ray Kelly announced at a security forum in Aspen, Colorado, on Saturday that Mayor Bloomberg will soon unveil the city's "Domain Awareness System," which the Associated Press describes as an "all-seeing" program that combines several streams of information to track criminals and potential terrorists. It's not clear yet if the Big Brother–y sounding system will change the way the department already surveils civilians or criminals, or Muslims in New Jersey, but Kelly said at the forum that the program combines citywide video surveillance with law enforcement databases. The city made the software in partnership with Microsoft; however, Office Anti-Terrorist Edition

TOP STORIES

- One NASA Employee's Lonely Celebration
- Video Proves Mitt Knows Whole Campaign Is a Lie
- Happy Birthday, Mr. President
- Name the People in This Obama Cabinet Photo

MOST POPULAR STORIES

Most Commented | Most Viewed

NYMAG.COM

1. At Least 20 Olympians Caught Fudging the Rules, Doping, or Dating Neo-Nazis
2. Deep Thoughts From Ryan Lochte
3. Why Washington Accepts Mass Unemployment

VULTURE.COM

1. Comedienne Tig Notaro Has Cancer and Did an Amazing Set About It

Scripts Partially Allowed, 9/15 (nymag.com, facebook.com, google.com, googleapis.com, google-analytics.com, fbcdn.net, twitter.com, googlesyndication.com, facebook.net) | <SCRIPT>: 97 | <OBJECT>: 0 Options...

YES

Address space changes how we must defend

- Automated defenses becoming the norm because of the address size and speed
- My bot can own your machine in 500 milliseconds; in that time you can set your coffee cup down." – Dan Geer

"We can do nothing but turn over an increasing percentage of the tasks of cybersecurity to machines. In a sense, they've [machines] already won." – Dan Geer

THE PROBLEM

Huge amounts of data feeds require automated analysis and response

- IPS, Stock trading programs, Air Traffic control
- We can trigger bad response by tweaking inputs

We want security in the real world

We haven't secured what we have already

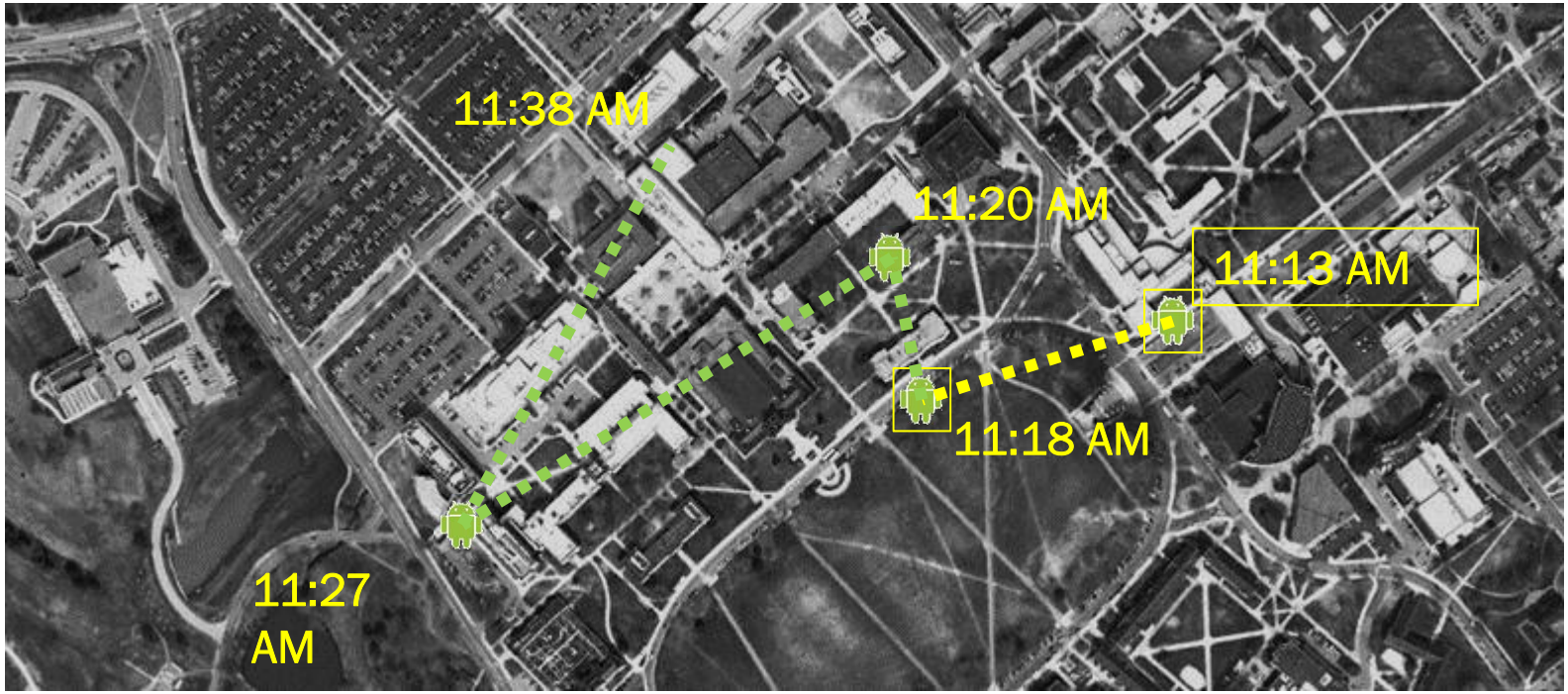
- Too expensive or institutional "laziness"

Have we examined these surveillance technologies for security flaws?

Security is a process not just cybersecurity

- Dealer service auto pickup example

IPV6 ADDRESS VULNERABILITY EXPLOITED



Simple tracking a host throughout campus

Filtering target traffic was trivial

IPV6 CHANGES THE RULES

IPv6 address size changes the rules

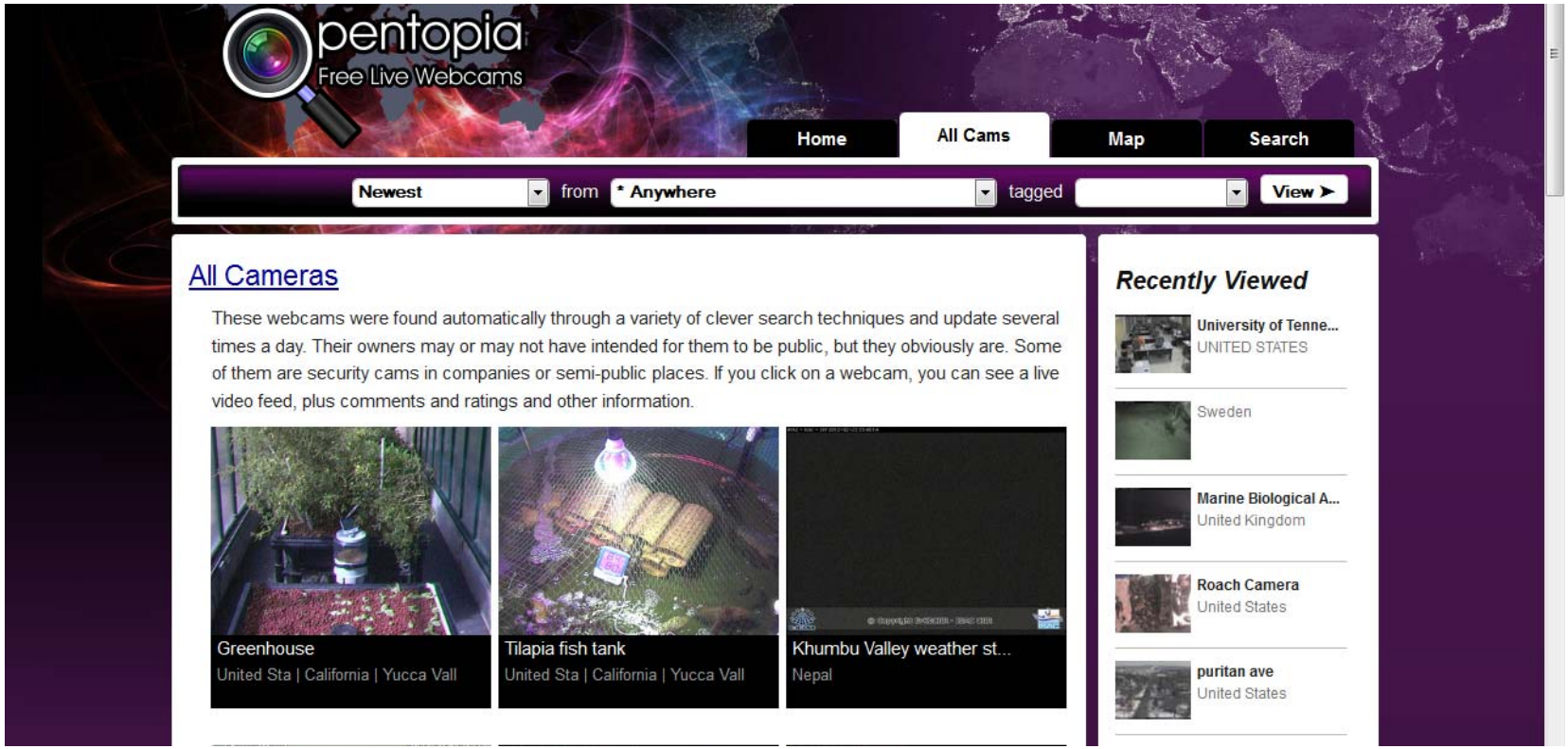
- 10**19 addresses in a single IPv6 subnet
- V4 Internet – 4 Billion addresses

DNS is REALLY critical

Sequential scanning of 1 IPv6 subnet takes ~10**10 years

WE'VE BECOME A SURVEILLANCE SOCIETY

SURVEILLANCE? WHY NOT? I'M NOT DOING ANYTHING WRONG



WE'RE AFRAID TO TRAVEL WITH OUR COMPUTERS.....

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS | STYLE | TRAVEL | JOBS | REAL ESTATE | AUTOS

Traveling Light in a Time of Digital Thievery

By NICOLE PERLROTH
Published: February 10, 2012

SAN FRANCISCO — When Kenneth G. Lieberthal, a China expert at the Brookings Institution, travels to that country, he follows a routine that seems straight from a spy film.

Enlarge This Image

Mary F. Calvert for The New York Times

Mike McConnell, former director of national intelligence, said some of the government's computer systems had been infected.

He leaves his cellphone and laptop at home and instead brings "loaner" devices, which he erases before he leaves the United States and wipes clean the minute he returns. In China, he disables Bluetooth and Wi-Fi, never lets his phone out of his sight and, in meetings, not only turns off his phone but also removes the battery, for fear his microphone could be turned on remotely. He connects to the Internet only through an encrypted, password-protected channel, and copies and pastes his password from a USB thumb drive. He never types in a password directly, because, he said, "the Chinese are very good at installing key-logging software on your laptop."

What might have once sounded like the behavior of a paranoid is now standard operating procedure for officials at American government agencies, research groups and

RECOMMEND
TWITTER
LINKEDIN
COMMENTS (113)
SIGN IN TO E-MAIL
PRINT
REPRINTS
SHARE

Log in to see what your friends are sharing on nytimes.com.
Privacy Policy | What's This?
Log In With Facebook

What's Popular Now

Lives Forever Linked Through Kidney Transplant Chain 124

John Fairfax, Who Rowed Across Oceans, Dies at 74

Subscribe to Technology RSS Feeds

Technology News
Internet
Start-Ups
Business Computing
Companies
Bits Blog
Personal Tech
Pogue's Posts

MOST E-MAILED | MOST VIEWED

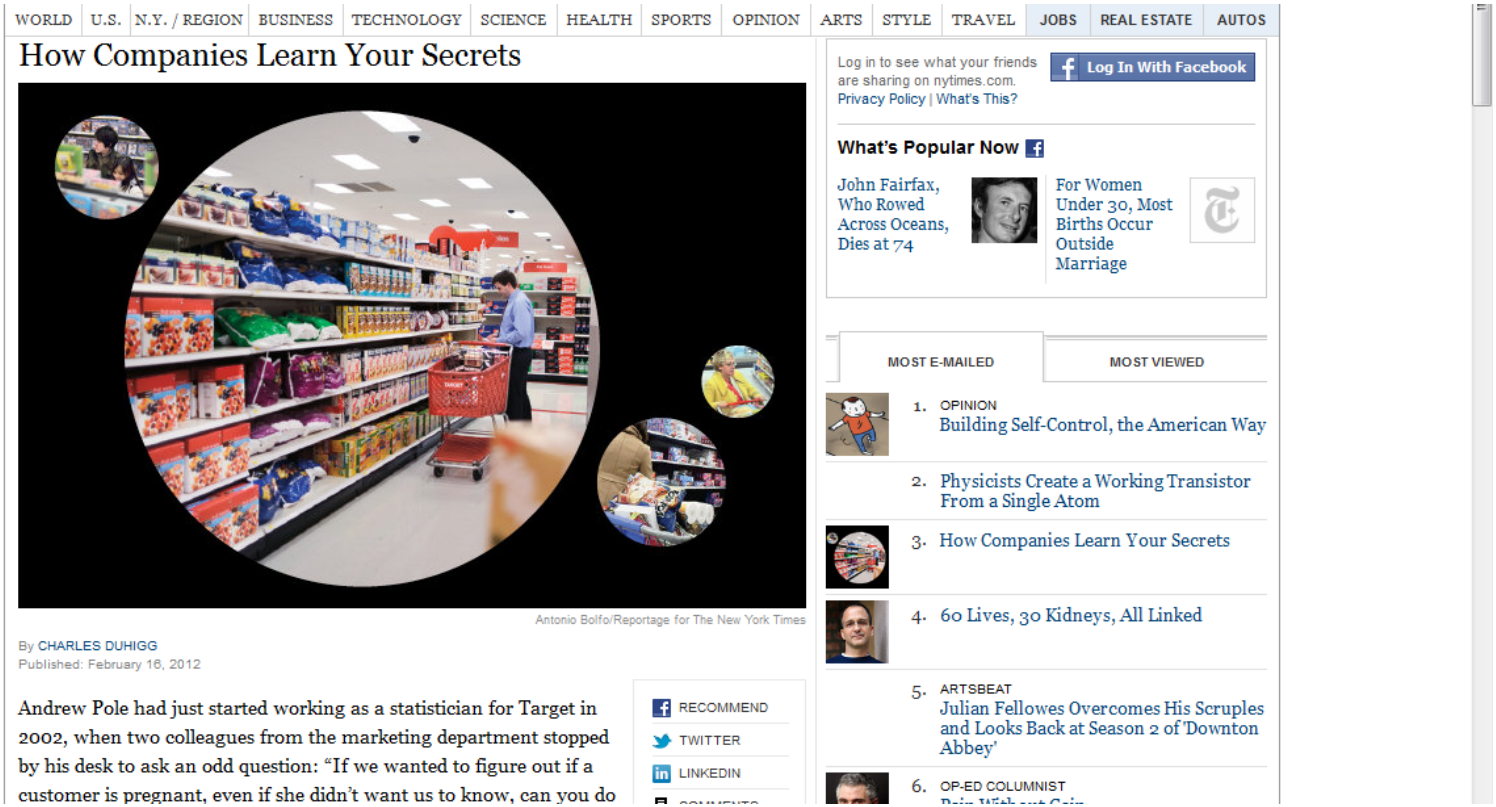
1. OPINION
Building Self-Control, the American Way

2. Physicists Create a Working Transistor From a Single Atom

3. How Companies Learn Your Secrets

4. 60 Lives, 30 Kidneys, All Linked

INDIVIDUALS VS. THE INTERNET



WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS | STYLE | TRAVEL | JOBS | REAL ESTATE | AUTOS

How Companies Learn Your Secrets

Antonio Bolfo/Reportage for The New York Times

By CHARLES DUHIGG
Published: February 16, 2012

Andrew Pole had just started working as a statistician for Target in 2002, when two colleagues from the marketing department stopped by his desk to ask an odd question: "If we wanted to figure out if a customer is pregnant, even if she didn't want us to know, can you do

RECOMMEND
TWITTER
LINKEDIN

Log in to see what your friends are sharing on nytimes.com.
Privacy Policy | What's This?
Log In With Facebook

What's Popular Now

John Fairfax, Who Rowed Across Oceans, Dies at 74

For Women Under 30, Most Births Occur Outside Marriage

MOST E-MAILED | MOST VIEWED

1. OPINION
Building Self-Control, the American Way

2. Physicists Create a Working Transistor From a Single Atom

3. How Companies Learn Your Secrets

4. 60 Lives, 30 Kidneys, All Linked

5. ARTSBEAT
Julian Fellowes Overcomes His Scruples and Looks Back at Season 2 of 'Downton Abbey'

6. OP-ED COLUMNIST

GOVERNMENTS VS. THE INTERNET

UK Edition | News | Reviews | Blogs | Mobile IT | History of the iPhone | White papers | Broadband | Windows 8 | Cloud | Security

ZDNet UK's special coverage on
Security

ZDNet UK / News and Analysis / Security / Security Threats

ISPs kept in dark about UK's plans to intercept Twitter

By Tom Espiner, ZDNet UK, 20 February, 2012 17:23 @tomespiner

NEWS The government has expanded its plans to store and monitor Twitter, Facebook and other personal web communication data, but these are being created without ISP involvement, according to an ISP representative body.

Under the plans, police and intelligence operatives will gain access to records of who has talked to whom on social networks, on instant messaging services, and in online multi-player games. The monitoring and storage are expected to be handled by ISPs, but the government's plans have not been officially shared with these companies, according to the Internet Service Providers Association (ISPA).

"It is important that proposals to update government's

Daily Newsletters

Sign up to ZDNet UK's daily newsletter.

Topics

Intercept, Interception Modernisation Programme, Communications Capabilities

Read this

Get ZDNet UK's daily newsletter

Enter your email address to sign up

Sign up now

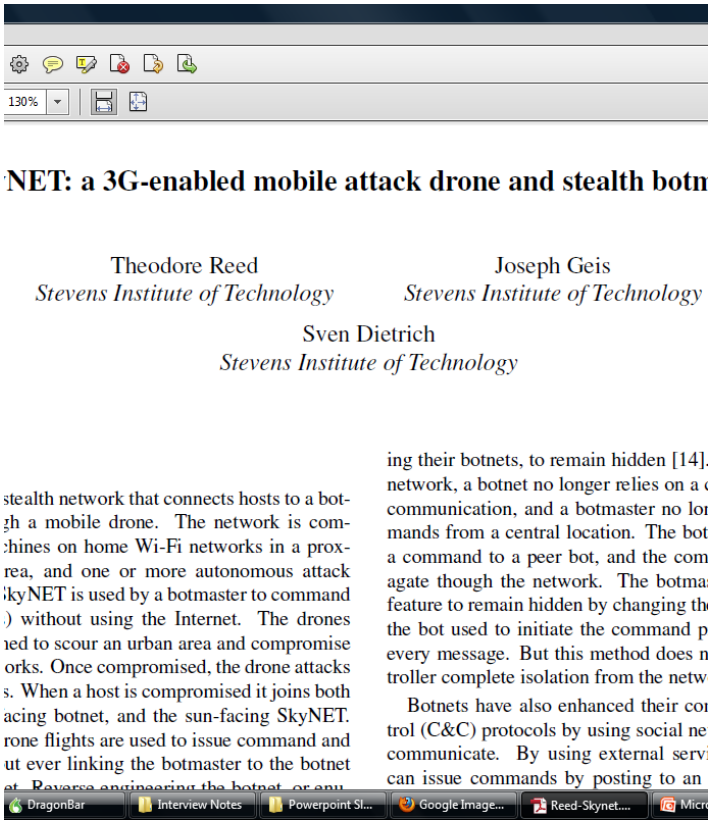
ZDNet UK Live

ZDNet writers looking like asses again, surprise. Apple can -- like any other individual or business in the world -- play favorites. You, yourself,...

6 minutes ago by Gemma81 on Apple briefs bloggers, blanks New York Times

So it kind of works like this. Back in the day when Jack was the technical guy over at the

SKYNET – IT'S BEING BUILT



130%

NET: a 3G-enabled mobile attack drone and stealth botn

Theodore Reed
Stevens Institute of Technology

Joseph Geis
Stevens Institute of Technology

Sven Dietrich
Stevens Institute of Technology

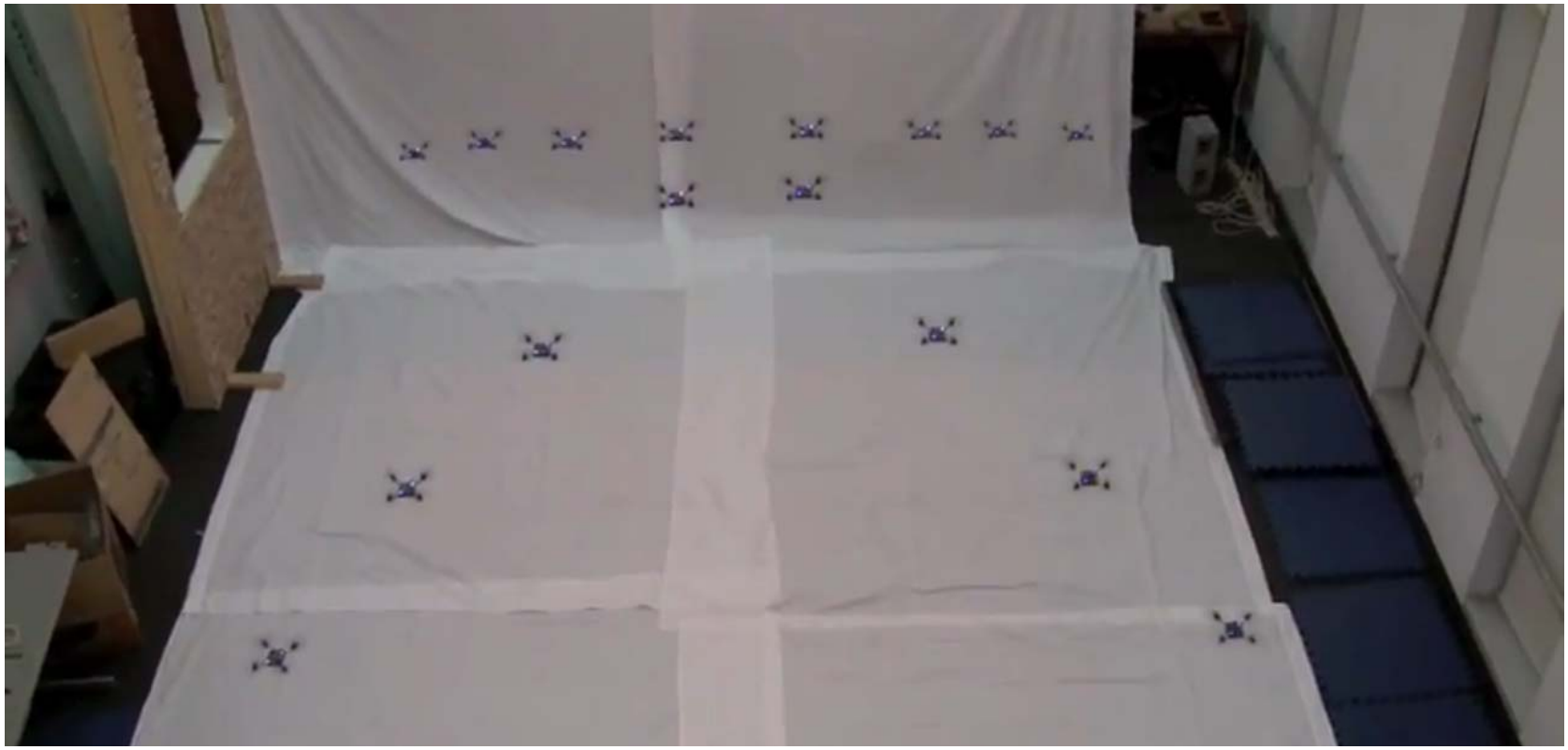
stealth network that connects hosts to a bot-
gh a mobile drone. The network is com-
chines on home Wi-Fi networks in a prox-
rea, and one or more autonomous attack
kyNET is used by a botmaster to command
) without using the Internet. The drones
ed to scour an urban area and compromise
orks. Once compromised, the drone attacks
s. When a host is compromised it joins both
acing botnet, and the sun-facing SkyNET.
rone flights are used to issue command and
ut ever linking the botmaster to the botnet

ing their botnets, to remain hidden [14].
network, a botnet no longer relies on a
communication, and a botmaster no lo
mands from a central location. The bot
a command to a peer bot, and the com
agate though the network. The botma
feature to remain hidden by changing th
the bot used to initiate the command p
every message. But this method does n
troller complete isolation from the netw

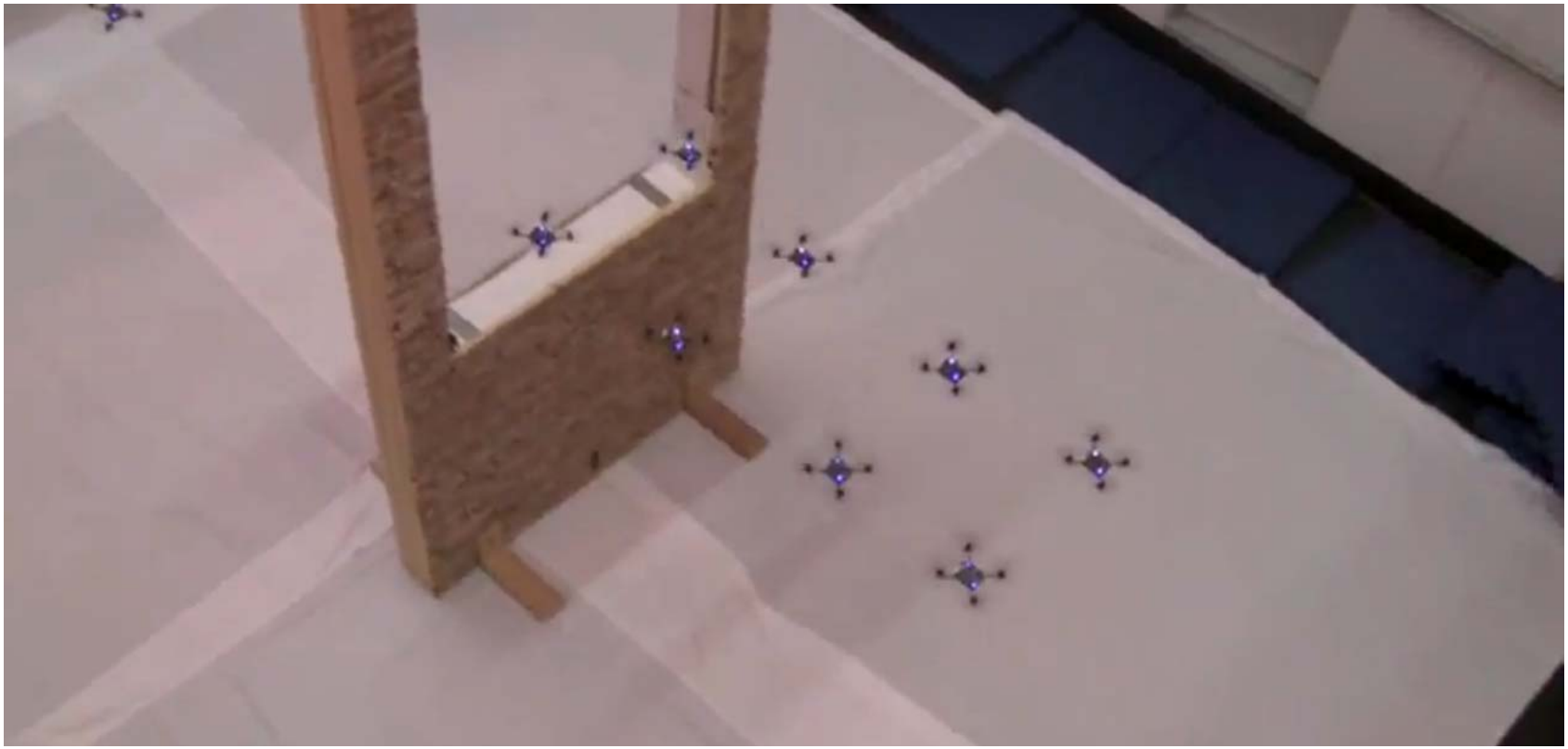
Botnets have also enhanced their co
trol (C&C) protocols by using social ne
communicate. By using external serv
can issue commands by posting to an

DragonBar | Interview Notes | Powerpoint Sl... | Google Image... | Reed-Skynet.... | Micr

DRONE SWARMS



ATTACK OF THE SWARMS



THEN ED ASKED ME:

"Do you ever wonder if what we [security professionals] are building is the future surveillance society and what we are doing is evil?" He then asked "When you talk to your grandchildren, will you be able to tell them what you built?“

Things that make you go “hmmmmm…….”

SOLUTIONS

Do something to fix the problem rather than measure compliance

Attach security riders to software purchase orders

- Is the product vulnerable to OWASP Top 10, SQL Injection, XSS, etc.?

Design security into systems.

- Not convenient for users? Tough.

Beware of the cloud if it's outside your "border"

- How does the cloud vendor deal with the 14 domains found at the Cloud Security Alliance's Security Guide ? https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Train your staff at their level or expertise

- User->MGT->technical staff

CONTACT INFORMATION

Randy Marchany

VA Tech IT Security Office & Lab

1300 Torgersen Hall

VA Tech

Blacksburg, VA 24060

540-231-9523

marchany@vt.edu

http://security.vt.edu

Twitter: @randymarchany

Blog: randymarchany.blogspot.com