Future Trends in Security

Steven M. Bellovin

`smb@cs.columbia.edu`

`http://www.cs.columbia.edu/~smb`

Department of Computer Science

Columbia University

Past, Present, Future

"Progress, far from consisting in change, depends on retentiveness. When change is absolute there remains no being to improve and no direction is set for possible improvement: and when experience is not retained, as among savages, infancy is perpetual. Those who cannot remember the past are condemned to repeat it. In the first stage of life the mind is frivolous and easily distracted, it misses progress by failing in consecutiveness and persistence. This is the condition of children and barbarians, in which instinct has learned nothing from experience."

George Santayana

The Past

- Conventional wisdom: “the folks who invented the Internet didn’t think about security; that’s why we have problems today”
- Reality: they did think about security, albeit somewhat incorrectly
- More reality: most of today’s problems have nothing to do with their (allegedly) bad decisions
- Let’s look back before we look ahead

The Original Vision

- The Internet is a pure pipe
- At least some nets are closed communities (classified nets still are)
- All it does is carry traffic; it has no life of its own
- "Highway robbery" doesn't mean you've stolen a part of the roadway

Early Hacking

- Early hackers claimed to be — and were — just curious
- First: only a small group had access back then
- There was no money to steal
- There weren't any corporate or military secrets online, either
- Most computer crime back then was committed by insiders — because few others had access. . .

Enter Al Gore

- The federal government loosened the restrictions on who could connect to the Internet
- Tim Berners-Lee invented the World-Wide Web, making some things much easier to do
- Companies connected, and started doing business
- Many more users connected, people who were not researchers or graduate students
- The stage was set. . .

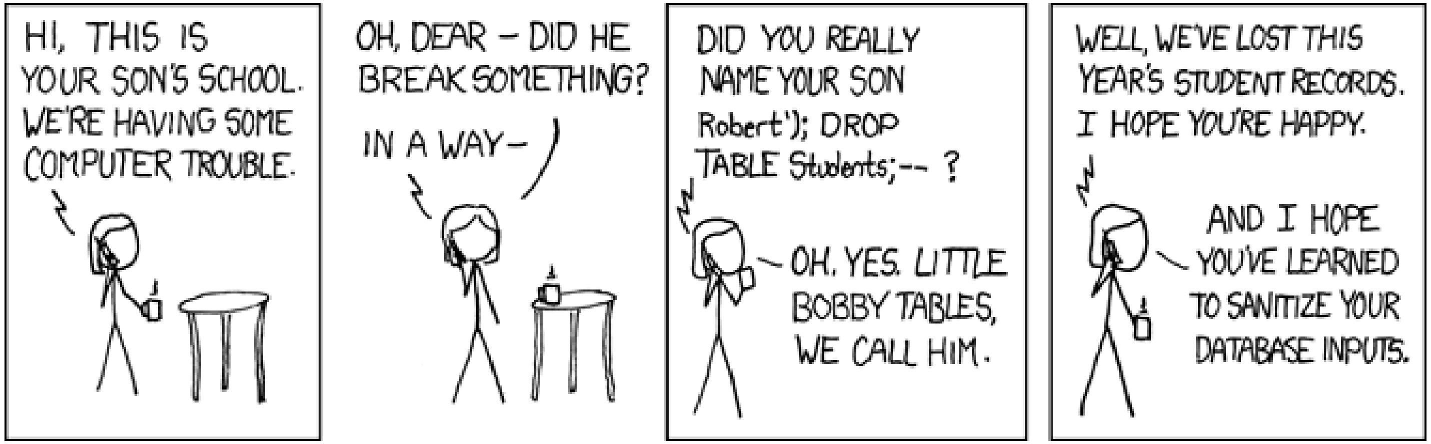
Joy-Hacking

- Primarily vandalism
- Primarily known techniques such as buffer overflows
- Rumors of more serious attacks. . .

Today

- Hacking for profit
- The spammers pay the hackers
- So does organized crime
- New holes being found by hackers
- Popular techniques: disassemble Microsoft patches; buffer overflow; SQL injection

SQL Injection


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

(From `http://xkcd.com/327/`)

“It’s Tough to Make Predictions, Especially About the Future”

- Governments (*many* governments!)
- Industrial spies
- High-end results for high-end customers. . .
- Old attacks refined
- Broad-spectrum attacks

It’s Not Just the Computer

- Combine physical or social attacks with technical measures
- Example: U3 flash disks in the parking lot
- Example: “spear-phishing”
- Example: other targets, like routers

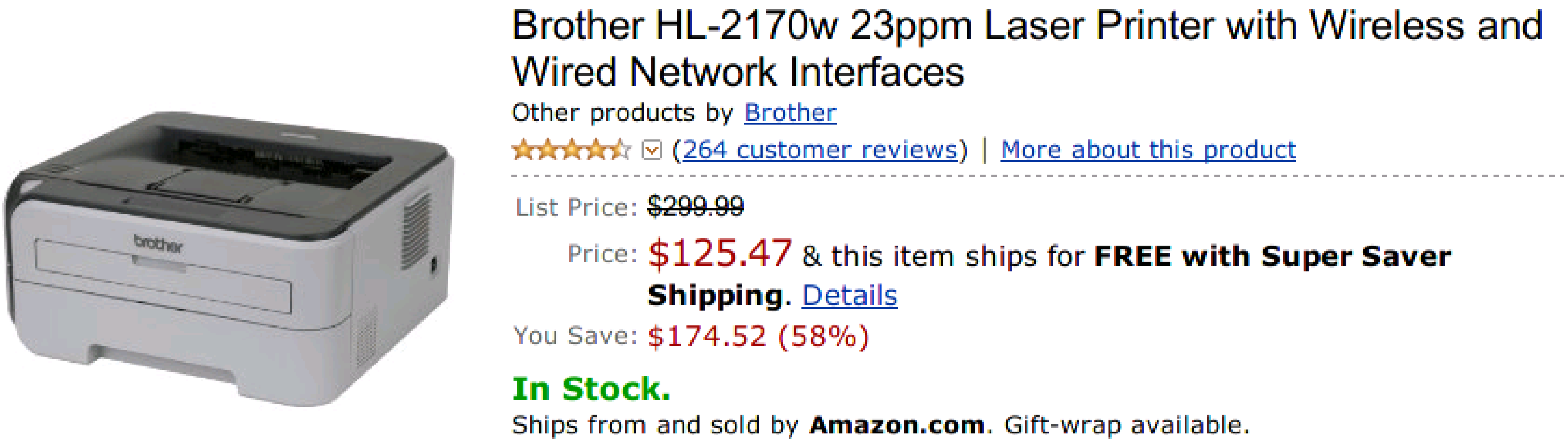
The Human Element

- We need systems that are human-friendly instead of human-hostile
- We need systems that are human-comprehensible
- We need systems that don't have normal modes of operation indistinguishable from an attack

What's a Computer?

- Cars have *many* microprocessors; increasingly, they have network links
- Implantable medical devices are controlled by software that your doctor can update
- Some thermostats are linked to the Internet today. Can a burglar learn that a house is empty by polling the temperature setting?
- Imagine new firmware in a networked printer that sent copies of all your documents to Someone

Printers?



Brother HL-2170w 23ppm Laser Printer with Wireless and Wired Network Interfaces

Other products by Brother

★★★★☆ (264 customer reviews) | More about this product

List Price: ~~$299.99~~

Price: $125.47 & this item ships for **FREE with Super Saver Shipping**. Details

You Save: $174.52 (58%)

In Stock.

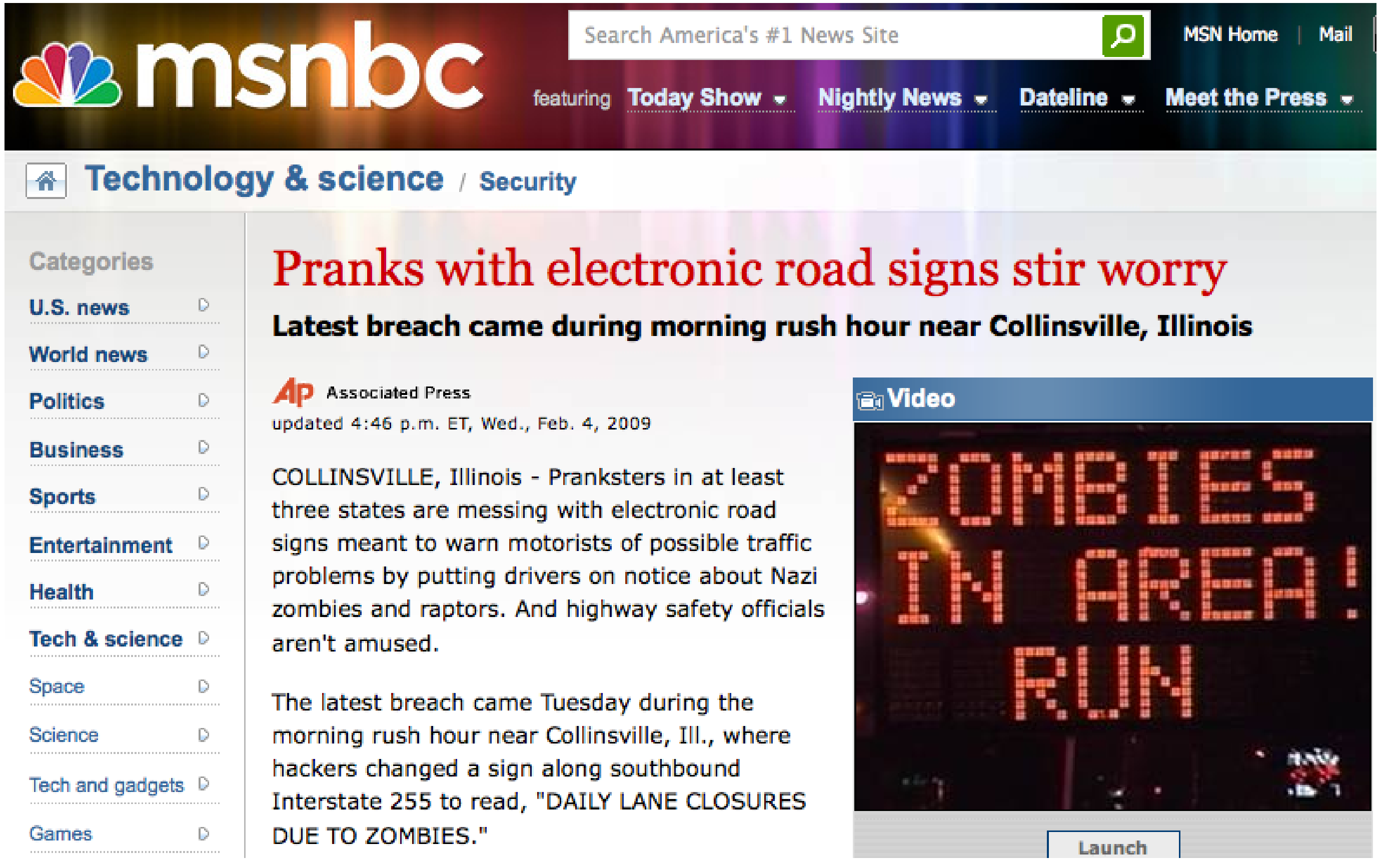
Ships from and sold by **Amazon.com**. Gift-wrap available.

Note: the first attack I know of against a programmable printer dates to about 1989. . .

Supply Chain Attacks

- Where does your hardware come from? The chips? The software?
- What if there are bad guys in the supply chain?
- What if the bad guys are governments?

Infrastructure?



Pranks with electronic road signs stir worry

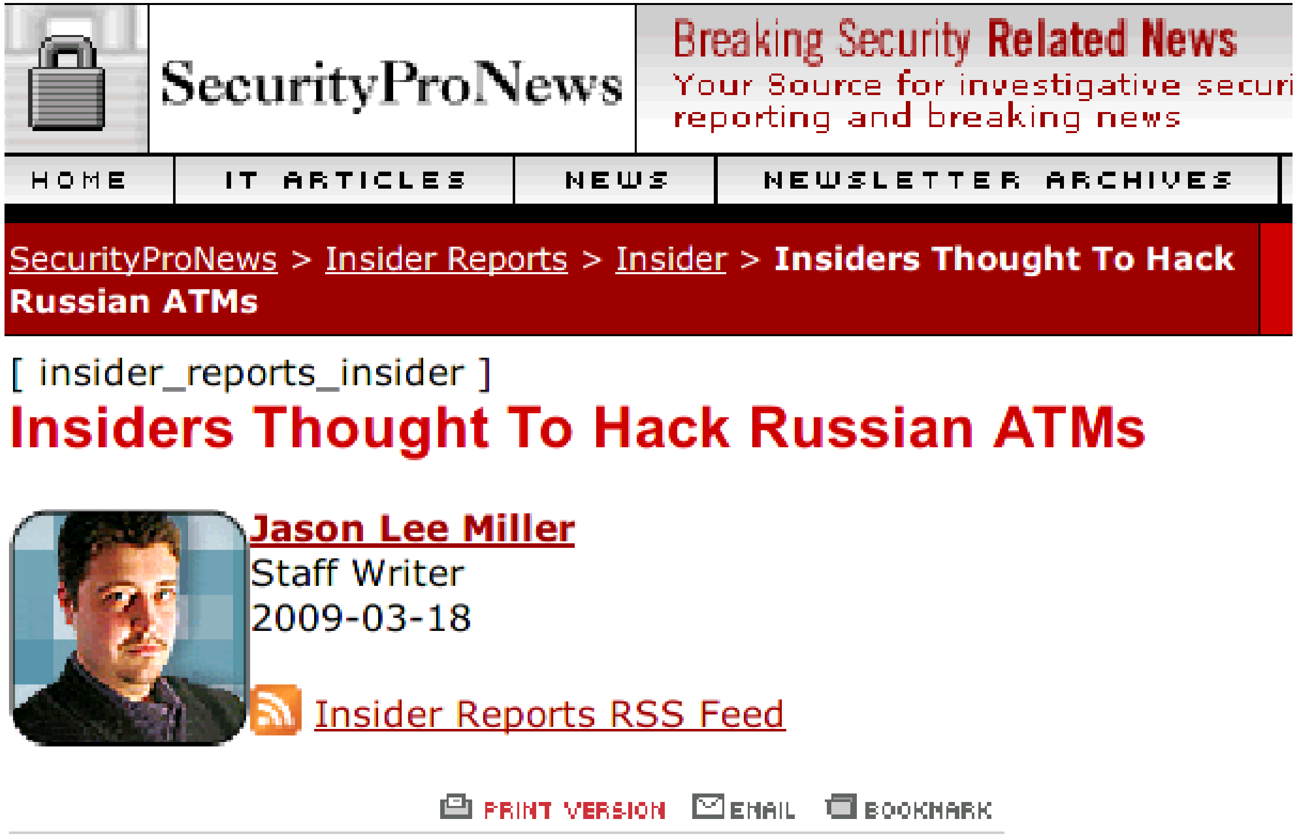
Latest breach came during morning rush hour near Collinsville, Illinois

AP Associated Press
updated 4:46 p.m. ET, Wed., Feb. 4, 2009

COLLINSVILLE, Illinois - Pranksters in at least three states are messing with electronic road signs meant to warn motorists of possible traffic problems by putting drivers on notice about Nazi zombies and raptors. And highway safety officials aren't amused.

The latest breach came Tuesday during the morning rush hour near Collinsville, Ill., where hackers changed a sign along southbound Interstate 255 to read, "DAILY LANE CLOSURES DUE TO ZOMBIES."

Hacked ATMs



SecurityProNews
Breaking Security Related News
Your Source for investigative securi
reporting and breaking news
HOME
IT ARTICLES
NEWS
NEWSLETTER ARCHIVES

SecurityProNews > Insider Reports > Insider > **Insiders Thought To Hack Russian ATMs**

[insider_reports_insider]

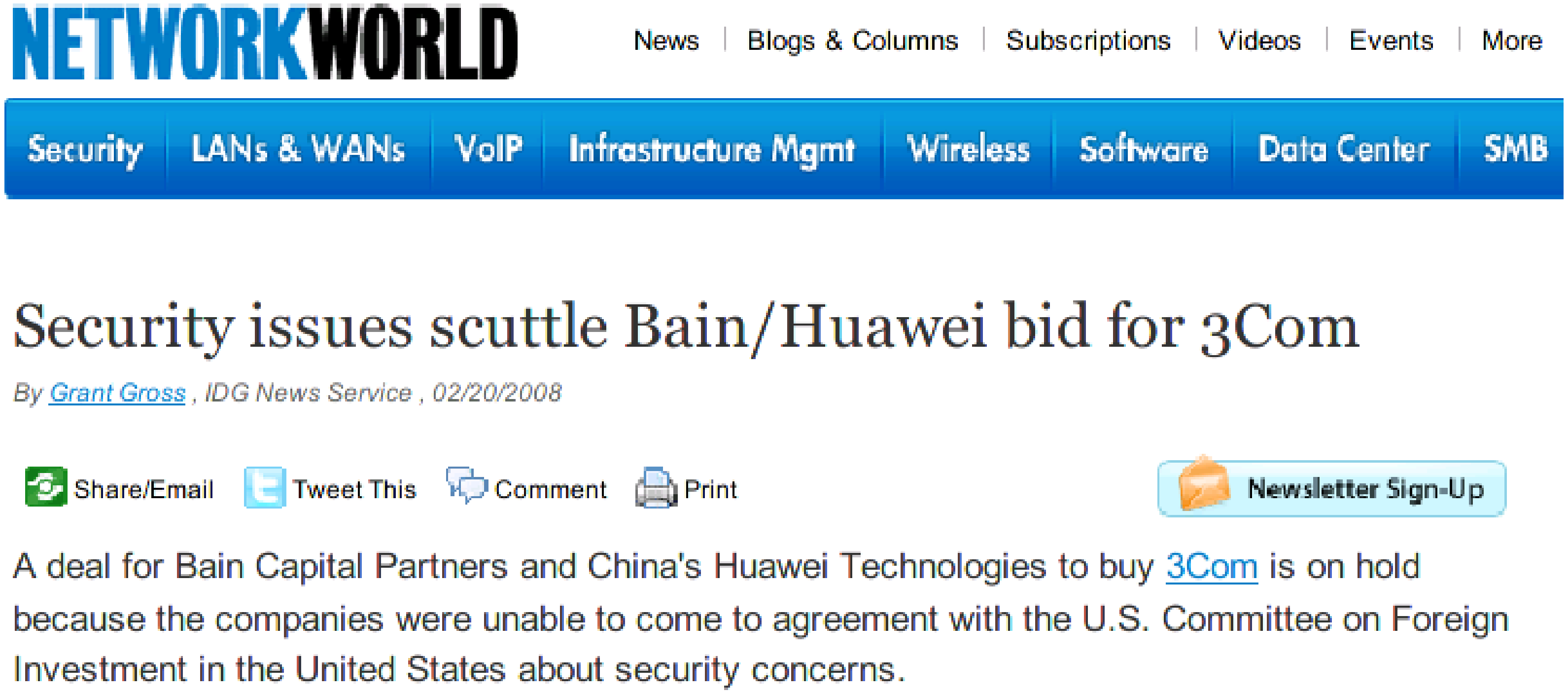
Insiders Thought To Hack Russian ATMs

Jason Lee Miller
Staff Writer
2009-03-18

Insider Reports RSS Feed

PRINT VERSION
EMAIL
BOOKMARK

Governments



Security issues scuttle Bain/Huawei bid for 3Com

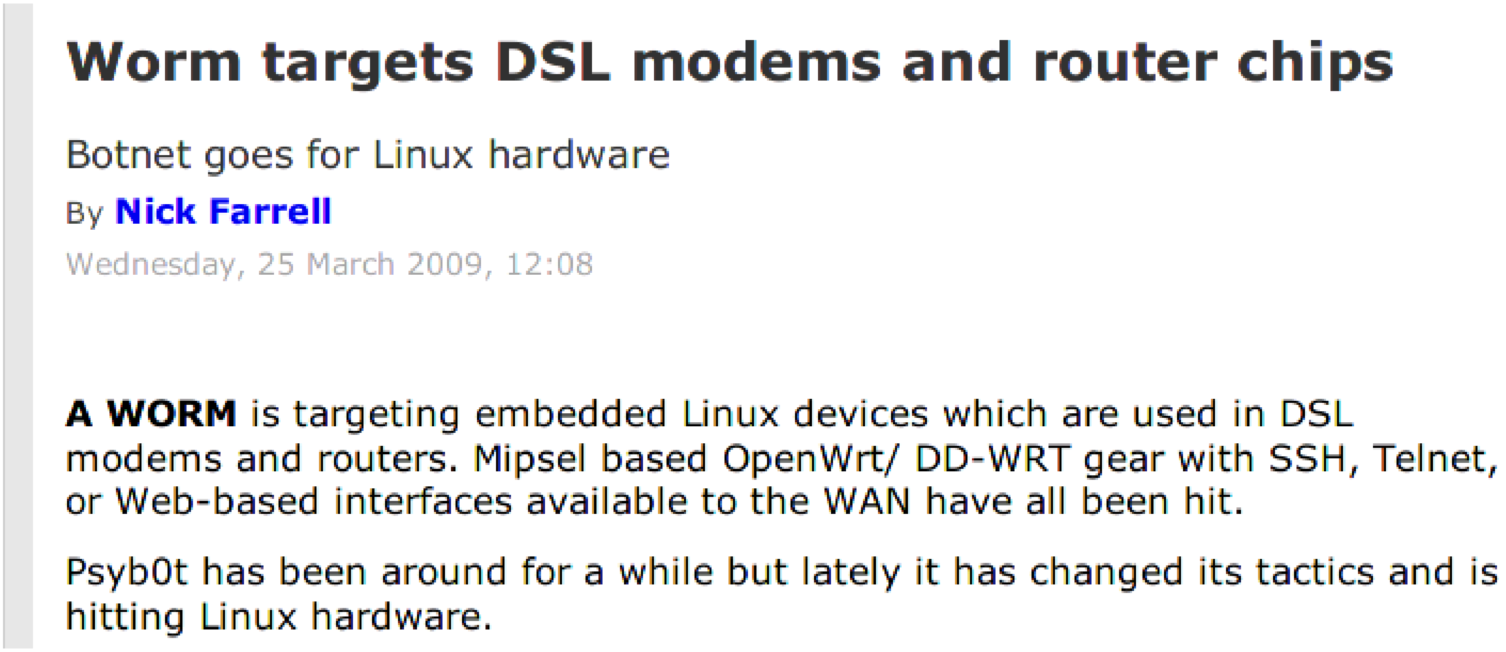
By Grant Gross , IDG News Service , 02/20/2008

A deal for Bain Capital Partners and China's Huawei Technologies to buy 3Com is on hold because the companies were unable to come to agreement with the U.S. Committee on Foreign Investment in the United States about security concerns.

New Hacks

- The bad guys are getting *really* good
- They're selling new attack technology — exploits are worth money
- They're looking beyond the desktop and beyond the server rack

Hacking Routers



Worm targets DSL modems and router chips

Botnet goes for Linux hardware

By **Nick Farrell**

Wednesday, 25 March 2009, 12:08

A WORM is targeting embedded Linux devices which are used in DSL modems and routers. Mipsel based OpenWrt/ DD-WRT gear with SSH, Telnet, or Web-based interfaces available to the WAN have all been hit.

Psyb0t has been around for a while but lately it has changed its tactics and is hitting Linux hardware.

(*The Inquirer*)

Blended Attacks

- Create an innocuous-seeming flaw in a chip
- Plant code to exercise the flaw in some application
- Distribute a particular data file — via a web page? via spam? — to run that piece of code
- Hard for an individual; conceivable for a nation-state

Selling Bugs

In the case of the Linux flaw, one agency offered him $10,000, while a second told him to name a price. When he said $80,000, his contact quickly agreed.

“The government official said he was not allowed to name a price, but that I should make an offer,” Miller told SecurityFocus. “And when I did, he said OK, and I thought, ‘Oh man, I could have gotten a lot more.’”

(*Security Focus*)

Mercenaries?

- Many hackers are already doing nasty things for pay
- Anonymity is easy on the Internet; attribution is hard
- For covert operations, deniability is always useful
- Will we see (anonymous) mercenary hackers working for governments?
- Will we return to letters of marque and reprisal?

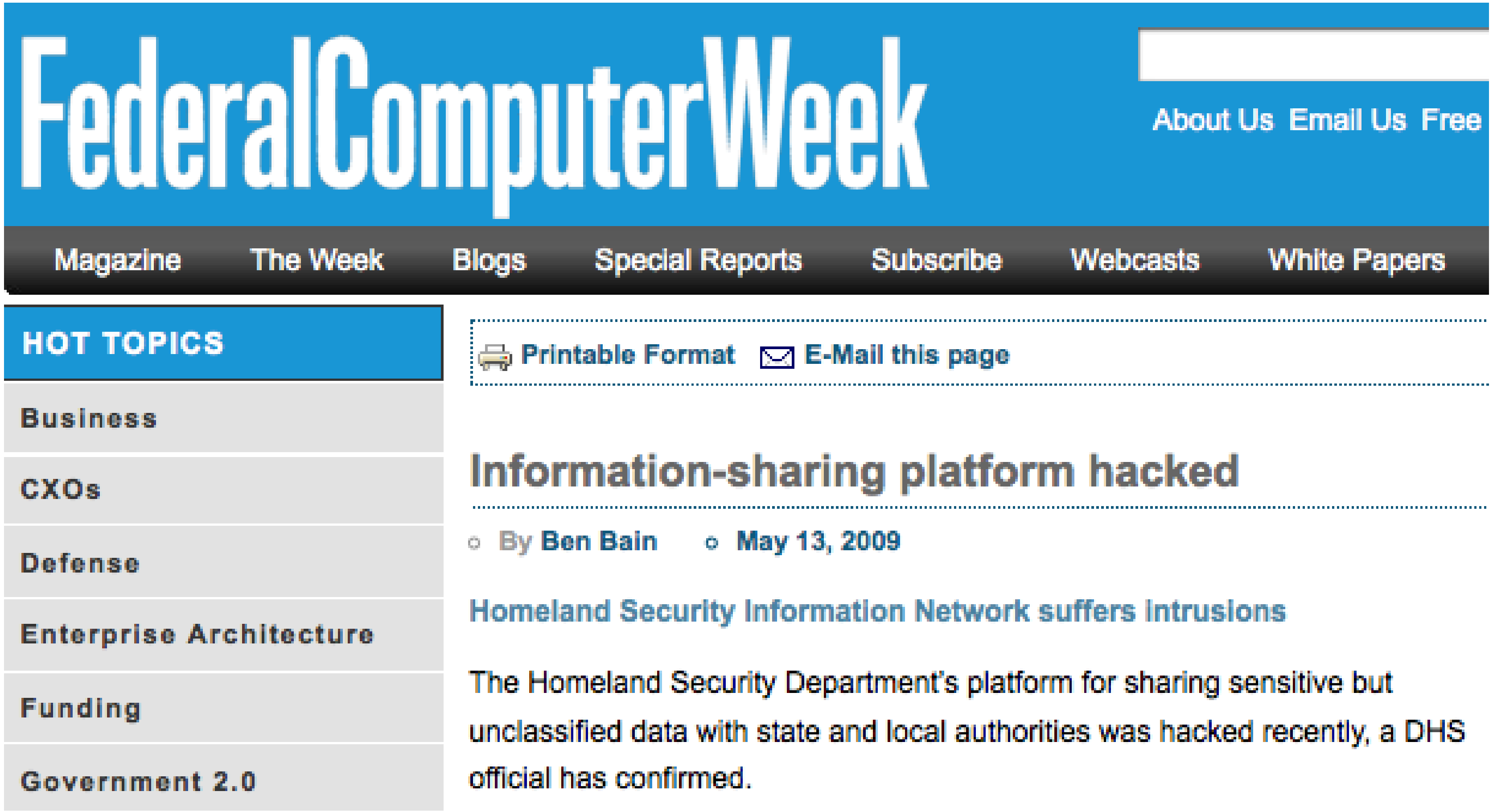
Target Selection

- We've already seen losses of tens of millions of dollars from cybercrime — could it go higher?
- What about stock market fraud based on stolen inside information?
- Theft of intellectual property for commercial reasons? (There are already claims that this is being done on behalf of governments.)

Implications

- Obviously, we cannot assume a benign environment
- We cannot even assume an ordinary enemy
- Many more systems have to be far more hardened than we had imagined, even a few years ago

It Can Happen to Anyone



Information-sharing platform hacked

○ By Ben Bain ○ May 13, 2009

Homeland Security Information Network suffers intrusions

The Homeland Security Department's platform for sharing sensitive but unclassified data with state and local authorities was hacked recently, a DHS official has confirmed.

Where Are We Going, and Why Are We in this Handbasket?

- The problem is (and was) buggy software
- Buggy software is not going away
- We have to understand that software is everywhere
- We have to accept that the bad guys are at least as good as we are at finding holes
- We cannot fight them on their own turf
- We have to find a way to *evade* attacks despite the certainty of security flaws

What to Do

- Accept that the risk exists
- Be humble about designs
- Complex functions need stronger protections
- Isolate subsystems

Optimizing for Security

- Optimize for speed last — but optimize for security from the beginning
- Security is a *systems* property; you do not achieve it by sprinkling on crypto or by adding a helping of firewalls
- Attackers don't go through strong security; they go around it
- "The key of strategy. . . is not to choose *a* path to victory, but to choose so that all paths lead to a victory."
  (Lois McMaster Bujold, *The Vor Game*)

No Shortcuts

- There is no royal road to security
- Eliminating — or avoiding — bugs is hard and expensive
- I don't think we need to get rid of the Internet – but we do need to get rid of the applications and operating systems
- Will we do better next time?
- Do the designers and programmers know geometry?

A New Hope?

- We may not be able to out-program the bad guys
- But — we can *out-design* them
- Computer crime is a matter of money — can we drive their costs too high?
- “Amateurs worry about algorithms; pros worry about economics”
- *We must avoid the single point of failure*