Lots of data is being collected
Many types of data

The Ultimate Net Monitoring Tool?
Posted by ScuttleMonkey on Wednesday May 17, 2006 @12:22PM from the corporations-striving-to-be-big-brother dept.

Wired News is reporting that the equipment found in the "secret" NSA room at AT&T was an elaborate device designed by Big Brother. Rather, it is a commercially available network packet product that any company could acquire. From the article:

"Anything that comes through a secret vice president of Narus, traffic, mails along with attachments of calls."

Schneier: Metadata Equals Surveillance
Posted by samzenpus on Monday September 23, 2013 @01:41PM from the a-rose-by-any-other-name dept.

Hugh Pickens DOT Com writes

"Bruce Schneier writes that lots of people discount the seriousness of the NSA's actions by saying that it's just metadata — after all the NSA isn't really listening in on everybody's calls — they're just keeping track of who you call. 'Imagine you hired a detective to eavesdrop on someone,' writes Schneier. 'He might plant a bug in their office. He might tap their phone.' That's the data. 'Now imagine you hired that same detective to surveil that person. The result would be details of what he did: where he went, who he talked to, what he looked at, what he purchased — how he spent his day. That's all metadata.' When the government collects metadata on the entire country, they put everyone under surveillance says Schneier. "Metadata equals surveillance; it's that simple."

The NSA Knows Who You've Called
Posted by Zonk on Thursday May 11, 2006 @06:55AM from the-at-least-i-know-i'm-free dept.

Magnifico writes

"USAToday is reporting on the National Security Agency's goal to create a database of every call ever made inside the USA. Aided by the cooperation of US telecom corporations, AT&T, Verizon and BellSouth, the NSA has been secretly collecting phone call records of tens of millions of Americans; the vast majority of whom aren't suspected of any crime. Only Qwest refused to give the NSA information because they were uneasy about giving information to the government without the proper warrants. The usefulness of the NSA's domestic phone call database as a counterterrorism tool is unclear."

Big Brother Wants Into VoIP At Any Cost
Posted by Zonk on Friday July 28, 2006 @12:36PM from the cracking-the-seal dept.

Wallaby fly-half writes

"An amendment to the CALEA law would make it easier for the government to monitor calls made over the internet. Ars Technica reports that the bill will put a hold on packet traffic, and places the job of filtering those streams..."

What Can You Find Out From Metadata?
Posted by samzenpus on Monday June 10, 2013 @03:10PM from the reading-between-the-lines dept.

cervesaebcraciator writes

"Snowden, apologists for the state security community are even 'glad' the NSA has been doing this. A 4 calls have remained private and it is only the much one can tell from interpersonal analysis can reveal far more. Duke sociologist shows how one father of the American Revolution is of social network analysis and only a limited..."
By lots of people
Been collected for a long time
Data comes from carriers

More Details Emerge On Domestic Spying Programs
Posted by kdawson on Saturday December 15, 2007 @07:36PM from the government-and-business-a-sittin'-in-a-tree dept.

The feed brings us this NYTimes story giving new details on the telecom carriers’ cooperation with secret NSA (and other) domestic spying programs. One revelation is that the Drug Enforcement Agency has been running a program since the 1990s to collect the phone records of calls from US citizens to Latin America in order to catch narcotics traffickers. Another revelation is what exactly the NSA asked for in 2001 that Qwest balked at supplying. According to the article, it was access to the company’s most localized communications switches, which primarily carry domestic calls.

AT&T Forwarding All Internet Traffic to NSA?
Posted by ScuttleMonkey on Friday April 07, 2006 @07:53AM from the will-it-never-end dept.

An anonymous reader writes

“SpamDailyNews is reporting that the Electronic Frontier Foundation (EFF) has filed a brief that claims AT&T has been forwarding internet traffic directly into the hands of the NSA. The brief was filed under seal (a procedure that allows only the judge and the litigants to view the document) in information. From the article: ‘More than just threatening iced to give the government secret, direct access to s communications is a threat to the Constitution itself. We are

Aussie Telco Telstra Agreed To Spy For America
Posted by Soulskill on Friday July 12, 2013 @05:48AM from the can't-even-trust-giant-soulless-corporations-anymore dept.

An anonymous reader writes

“Australian telecommunications giant Telstra has for a decade been storing huge volumes of electronic communications carried between Asia and America for surveillance by U.S. intelligence agencies. This includes not just the metadata, but the actual content of emails, online messages and phone calls. With the blessing of the Australian government Telstra agreed to route data through a ‘U.S. point of contact through a secure storage facility on U.S. soil that was staffed exclusively by U.S. citizens.’ The contract was prompted by Telstra's decision to expand its business in Asia by taking control of hundreds of kilometers of undersea telecommunications cables. The deal started under the Liberal Party and continued under Labor. The Greens have demanded an explanation.”
Data comes from transports

GCHQ Tapping UK Fiber-Optic Cables

An anonymous reader writes

*According to The Guardian, the UK government is tapping fiber-optic cables that carry global communications and gathering vast amounts of data. The British Government Communications Headquarters (GCHQ) has been sharing the data with its American counterpart, the NSA. The sheer scale of the agency's ambition is reflected in the titles of its two principal components: Mastering the Internet and Global Telecoms Exploitation, aimed at scooping up as much online and telephone traffic as possible. This is all being carried out without any form of public acknowledgement or debate. ... The documents reveal that by last year GCHQ was handling 600m "telephone events" each day, had tapped more than 200 fibre-optic cables and was able to process data from at least 46 of them at a time.*

NSA Tapping Underwater Fiber Optics

An anonymous reader submitted an interesting story about the NSA splicing fiber optics under water in order to eavesdrop on digital traffic. This happened years ago, so who knows what they’re doing today. Not surprisingly, apparently actually getting the tap is relatively easy. Sifting through the zillions of bits and finding something useful is a little trickier.
And data comes from cloud services

MS Handed NSA Access To Encrypted Chat & Email
Posted by timothy on Thursday July 11, 2013 @02:41PM
from the tangled-web-they-weave dept.

kaptink writes with the latest revelation from Edward Snowden:
"Microsoft helped the NSA to circumvent its encryption to address concerns that the agency would be unable to intercept web chats on the new Outlook.com portal. The agency already had pre-encryption stage access to email on Outlook.com, including Hotmail. This year, the FBI is allowing the NSA easier access via Prism to its cloud stor which now has more than 250 million users worldwide. Microsoft also worked with the Intercept Unit to 'understand' potential issues with a feature in Outlook.com. The software create email aliases. Skype, which was bought by Microsoft in October 2011 as part of its efforts to enter the intelligence agencies last year to allow Prism to collect video of conversations. Material collected through Prism is shared with the FBI and CIA.

Microsoft's Cooperation With NSA Either Voluntary, Or Reveals New Legal Tactic
Posted by timothy on Saturday July 13, 2013 @06:28AM
from the man-in-the-middle-attack dept.

holy_calamity writes
"It re-engineered its online services to assist NSA surveillance programs, the
either acting voluntarily, or under a new kind of court order, reports MIT Technology
when the laws were believed to shelter companies from being forced to modify their
surveillance, but experts say the Foreign Intelligence Surveillance Court may now
separation. Microsoft's statement about its cooperation with NSA surveillance
I'm clear whether it acted under legal duress, or simply decided that to helping out
in its best interest."

When the NSA Shows Up At Your Internet Company
Posted by samzenpus on Sunday July 21, 2013 @02:04PM
from the when-the-man-comes-around dept.

Frosty Piss writes
"When people say the feds are monitoring what people are doing online, what does that mean? How
does that work? When, and where, does it start? Pete Ashdown, CEO of XMission, an internet
service provider in Utah, knows. He received a Foreign Intelligence Service Act (FISA) warrant in
2010 mandating he let the feds monitor one of his customers, through his facility. He also received
a broad gag order. Says Mr. Ashdown, 'I would love to tell you all the details, but I did get
an order... These programs that violate the Bill of Rights can continue because people can't
say, This my experience, this is what happened to me, and I don't think it is right.' In this
Mr. Ashdown tells us about the equipment the NSA installed on his network, and what he
did."

Microsoft Funded by NSA, Helps Spy on Win Users?
Posted by Roblimo on Saturday February 19, 2000 @08:07AM
from the deep-dark-conspiracy-theories dept.

OppenNerd writes
"A French intelligence report has accused U.S. secret agents of working with computer giant
Microsoft to develop software allowing Washington to spy on communications around the world.
According to the report, 'It would seem that the creation of Microsoft was largely supported, not
least financially, by the NSA, and that IBM was made to accept the (Microsoft) MS-DOS operating
system by the same administration.'"
Really, really, really, lots of data
Includes active attacks

**Australian Spy Agency Seeks Permission To Hack Third-Party Computers**

Posted by Soulkiller on Saturday January 12, 2013 @05:01PM from the you-are-doing-it-wrong dept.

New submitter LordLucless writes

"ASIO, Australia's spy agency, is pushing for the ability to lawfully hijack peoples' computers — even if they are not under suspicion of any crime. They seek the ability to gain access to a third party's computer in order to facilitate gaining access to the real target — essentially using any person's personal computer as a proxy for their hacking attempts. The current legislation prohibits any action by ASIO that, among other things, interferes with a person's legitimate use of their computer. Conceivably, over-turning this restriction would give ASIO the ability, they say these changes are needed for national security reasons.

---

**GCHQ Created Spoofed Linkedin and Slashdot Sites To Serve Malware**

Posted by samzenpus on Sunday November 10, 2013 @04:25PM from the careful-what-you-click dept.

An anonymous reader writes

"Ars Technica reports how a Snowden leak shows British spy agency GCHQ spoofed LinkedIn and Slashdot so as to serve malware to targeted employees. From the article: Der Spiegel suggests that the Government Communications Headquarters (GCHQ), the British sister agency to the NSA, used spoofed versions of LinkedIn and Slashdot pages to serve malware to targets. This type of attack was also used to target "nine salaried employees" of the Organization of Petroleum Exporting Countries (OPEC), the global oil cartel."

---

**NSA Infected 50,000 Computer Networks With Malicious Software**

Posted by Unknown Lamer on Saturday November 23, 2013 @03:22PM from the pretty-sure-that's-illegal dept.

rtoz writes

"The American intelligence service — NSA — infected more than 50,000 computer networks worldwide with malicious software designed to steal sensitive information, documents provided by former NSA-employee Edward Snowden show."
Let’s be organized

• Need to fit all these attacks into a threat model
• Ensure that our work covers all the attacks
• … and we don’t work on things that don’t help
Passive attacker

- Attacker can listen to communications
- Same old attack we know and love
- **Pervasive** attack can *correlate* communications
Passive attacker

- **Mitigation**: Hide information on the wire
  - Minimization: Just don’t send the information
  - Encryption: Render the information unintelligible
  - Anonymization: Render the information intelligible
Active attacker

- Attacker can observe and modify communications
- **Pervasive** attacker in the network core can attack more sessions (e.g., by winning race conditions)
- **Pervasive** attackers are often in a good position to acquire bogus (but valid) credentials
Active attacker

- **Mitigation**: Make sure you’re talking to who you think you are
  - Authentication technologies (e.g., PKIX, DANE)
  - Improve information about who to trust
  - Key pinning, Certificate Transparency, DANE
Aside: Collaboration

• A legitimate actor giving help to the attacker
  • Static: One-time help (e.g., private key)
  • Dynamic: Ongoing, per-session help
  • Content: The desired content itself

• Witting or unwitting
  • Your IT can collaborate on your behalf

• Real or virtual
  • Hand over key data or make it predictable
Static key exfiltration

- Collaborator provides attacker with long-lived keys

- Mitigation: Use PFS to require per-session keys
Dynamic key exfiltration

- Collaborator provides attacker with per-session keys

- Mitigation: Use PFS to require per-session keys
Content exfiltration

- Collaborator provides user information to attacker
- Especially common in messaging & cloud apps
**Content exfiltration**

- Mitigation: Deny the server access to information
  - End-to-end security on messages (e.g., S/MIME, PGP)
  - Avoid concentration information on a few servers
Summary

• Five main attack classes
  • Pervasive passive attack [metadata, correlation]
  • Pervasive active attack [access in the network core]
  • Static key exfiltration
  • Dynamic key exfiltration
  • Content exfiltration

• In reality, attackers will do all of these

• Technology can increase the cost of attackers getting what they want
  • Technology cost (passive → active)
  • Risk of exposure (static → dynamic, target dispersal)
Discussion