Pervasive Attack: A Threat Model

draft-barnes-pervasive-problem-00

Richard Barnes
Bruce Schneier
Cullen Jennings
Ted Hardie

Lots of data is being collected

Congress concerned about Echelon

Posted by **sengan** on Friday June 04, 1999 @01:10PM
from the who-approved-its-financing? dept.

Congress is concerned about Echelon invading the privacy of US citizens. Indeed, for the
history, the NSA has refused to supply the House Permanent Select Committee with docu
Echelon.

No Upper Bound On Phone Record Collection, Says NSA

Posted by **timothy** on Thursday September 26, 2013 @03:03PM
from the don't-write-a-blank-check-to-the-government dept.

PCWorld reports that

lance court has given the National Security Agency no limit on the number of U.S.
s it collects in the name of fighting terrorism, the NSA director said Thursday. The
collect all U.S. telephone records and put them in a searchable 'lock box' in the
al security, General Keith Alexander, the NSA's director, told U.S. senators."

ust metadata, until it isn't. (Your row in the NSA database may already be getting
home in Utah.)

U.S. Gov To Spider Internet

Posted by **Zonk** on Thursday February 09, 2006 @08:56AM
from the dog-house-farm-house-chicken-house-outhouse dept.

HopeSeekr of xMule writes

> "Perhaps as one of the first high profile uses of Alexa's WebSearch Platform, the U.S. government
> plans to search, link and reference every news site, blog and email on the Internet,
> sophisticated AI codenamed ADVISE to do the correlations. Unlike traditional datav
> Echelon, ADVISE aims to find terrorists before they strike and even deduce their m
> wanting to commit their crimes. Part of the breakthrough is a way for humans to vie
> holographic images with tech recently used at the Superbowl."

Snowden Strikes Again: NSA Mapping Social Connections of US Citizens

Posted by **Soulskill** on Sunday September 29, 2013 @06:21AM
from the raise-your-hand-if-you-are-surprised dept.

McGruber writes

nes is reporting on yet another NSA revelation: for the last three years, the
Agency has been exploiting its huge collections of data to create sophisticated
nericans' social connections that can identify their associates, their locations at
traveling companions and other personal information. 'The agency can augment
is data with material from public, commercial and other sources, including bank
nformation, Facebook profiles, passenger manifests, voter registration rolls and
mation, as well as property records and unspecified tax data, according to the
do not indicate any restrictions on the use of such "enrichment" data, and several
ma administration officials said the agency drew on it for both Americans and
emorandum, NSA analysts were 'told that they could trace the contacts of

US Director of National Intelligence Admits He Was Wrong About Data Collection

Posted by **Soulskill** on Wednesday July 03, 2013 @04:31AM
from the promoted-to-director-of-the-obvious dept.

Gunkerty Jeb writes

> "In a highly unusual move, James Clapper, the director of national intelligence, said Tuesday that
> he misspoke when he told a Congressional committee in March that the National Security Agency
> does not collect data on millions of Americans. Clapper said at the time that the agency does not
> do so 'wittingly,' but in a letter to the chair of the Senate Select Committee on Intelligence, Clapper
> admitted this statement was 'erroneous.' Clapper, the top U.S. intelligence official, has been quite
> vocal in his defense of the NSA's now-public surveillance programs such as PRISM and the
> metadata collection program. In statements published shortly after the leak of classified documents

Many types of data

Schneier: Metadata Equals Surveillance

Posted by **samzenpus** on Monday September 23, 2013 @02:41PM
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 that it's just metadata — after all the NSA isn't really listening in on every keeping track of who you call. 'Imagine you hired a detective to eavesdrc Schneier. 'He might plant a bug in their office. He might tap their phone.' imagine you hired that same detective to surveil that person. The result did: where he went, who he talked to, what he looked at, what he purchas day. That's all metadata.' When the government collects metadata on the everyone under surveillance says Schneier. 'Metadata equals surveillanc

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
> mporarily store some packet traffic. Ars Technica reports that the 'bill will put
> to buffer packet streams, and places the job of filtering those streams

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 wasr elaborate device designed by Big Brother. Rather, it is a commercially available network-a product that any company could acquire. From the article:

> "'Anything that comes throug
> vice president of Narus, a Mc
> mails along with attachments
> calls.'"

What Can You Find Out From Metadata?

Posted by **samzenpus** on Monday June 10, 2013 @03:10PM
from the reading-between-the-lines dept.

cervesaebraciator writes

> Snowden, apologists for the state security
> ome are even 'glad' the NSA has been doing this. A
> f calls have remained private and it is only the
> w much one can tell from interpersonal
> nt a 'modest encroachments on privacy?' It is easy
> made to and from a medical specialist could be
> analysis can reveal far more. Duke sociologist
> , shows how one father of the American Revolution
> ols of social network analysis and only a limited

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.'"

By lots of people

Australia Spying On Its Own

Posted by **timothy** on Tuesday February 12, 2002 @03:42AM
from the he-ain't-heavy-he's-big-brother dept.

AVIDLY INTERESTED writes:

Whistleblower Claims NSA Spied On Everyone, Targeted Media

Posted by **timothy** on Thursday January 22, 2009 @12:08PM
from the puzzle-palace dept.

JCWDenton writes

US Hacked Chinese University Network

Posted by **Soulskill** on Sunday June 23, 2013 @03:23AM
from the plot-thickens dept.

Canadian Spy Agency Snooped Travelers With Airport Wi-Fi

Posted by **Soulskill** on Friday January 31, 2014 @08:54AM
from the mapping-everyone's-hockey-allegiances dept.

Walking The Walk writes:

> "It seems the NSA isn't the only agency doing illegal domestic spying. According to a S
> document obtained by the CBC, Communications Security Establishment Canada (CSE
> apparently been tracking domestic travelers, starting from when they first use free Wi-F

NSA Cracked Into Encrypted UN Video Conferences

Posted by **timothy** on Sunday August 25, 2013 @10:28AM
from the for-the-greater-good dept.

McGruber writes

> "According to documents seen by Germany's Der Spiegel, the U.S. National Security Agency
> (NSA) successfully cracked the encryption code protecting the United Nations' internal
> videoconferencing system. NSA first breached the UN system in the summer of 2012 and, withi
> three weeks of initially gaining access to the UN system, the NSA had increased the number of
> such decrypted communications from 12 to 458. On one occasion, according to the report, while
> the American NSA were attempting to break into UN communications, they discovered the Chin
> were attempting to crack the encryption code as well."

French Gov't Runs Vast Electronic Spying Operation of Its Own

Posted by **timothy** on Thursday July 04, 2013 @12:06PM
from the but-it's-only-wafer-thin-metadata dept.

Freshly Exhumed writes with this news (quoting The Guardian):

> "France runs a vast electronic surveillance operation, intercepting and stocking data from citizens' phone and internet activity, using similar methods to the U.S. National Security Agency's Prism programme exposed by Edward Snowden, Le Monde has reported. An investigation by the French daily [en français; Google translation] found that the DGSE, France's external intelligence agency, had spied on the French public's phone calls, emails and internet activity. The agency intercepted signals from computers and phones in France as well as between France and other countries, looking not so much at content but to create a map of 'who is talking to whom,' the paper said."

Inside Echelon

Posted by **CmdrTaco** on Wednesday July 26, 2000 @08:59AM
piracy-theorists dept.

Revealed: How the UK Spied On Its G20 Allies At London Summits

Posted by **timothy** on Sunday June 16, 2013 @05:28PM
atte-sirs-and-madams? dept.

w, this is going to really set the cat amongst the pigeons once this gets around," an
reader links to a story at The Guardian about some good old fashioned friendly interception,
e-show version of what went on at recent G20 summits in London:

Britain Tapped Communications

Posted by **justin++** on Friday July 16, 1999 @05:45AM
from the actually-or-allegedly? dept.

The BBC news is reporting (thanks to aspodf for the link) that Channel 4 News alleges that the Ministry of Defence (MoD) has been intercepting all phone calls between Britain and Ireland for the last 10 years. A similar article in The Independent presents similar information as fact. Apparently, the tower was used to scan every single message between Britain and Ireland for certain key words (sort of like Echelon), and the tower is now up for sale by the MoD.

vikingpower writes

> "In the ever-longer wake of the NSA scandal, much-respected Dutch newspaper NRC today reveals, in English, as mandated by the gravity of the occasion, that the Dutch secret service, the AIVD, hacks internet forums. And yes, that is gross misconduct against Dutch law. The service, whose headquarters are in Zoetermeer, did not yet comment upon the divulgence of the document from Edward Snowden's collection. Incensed Dutch parliamentarians are calling for an enquiry."

Been collected for a long time

Government Wants to do Massive Internet Monitoring

Posted by **Roblimo** on Wednesday July 28, 1999 @07:10AM
from the all-they-want-to-do-is-protect-you- dept.

jht writes

> "Taking the Clinton Administration's electronic paranoia to new heights, this NY Times article details plans to have the FBI establish an infrastructure (called FIDNET) capable of monitoring all non-military public networks. And you were wondering why they're so down on encryption... The NSA is reviewing it now, with final rules expected in September. "

Uh,oh. This is potentially a Very Bad Thing. You may want to e-mail your Congressional Repres about it. (Free NYT online subscription required to read the article.)

NSA Had Domestic Call Monitoring Before 9/11?

Posted by **Zonk** on Sunday July 02, 2006 @04:57AM
from the they-have-the-high-end-magic-eight-ball dept.

MarkusQ writes

> "Bloomberg is reporting that, according to documents filed in the breach of privacy suit on behalf of Verizon and BellSouth, the NSA asked AT&T to set up its domestic call monitoring site seven months before the Sept. 11, 2001 attacks. Could it be that they were intending to monitor domestic calls (and internet traffic) all along, and the 'Global War on Terror' was just a convenient excuse when they got caught?"

From the article:

AT&T Maintains Call Database For the DEA Going Back To 1987

Posted by **samzenpus** on Monday September 02, 2013 @08:05AM
from the all-your-calls-are-belong-to-us dept.

Jah-Wren Ryel writes

> "Forget the NSA — the DEA has been working hand-in-hand with AT&T on a database of records of every call that passes through AT&T's phone switches going back as far as 1987. The government pays AT&T for contractors who sit side-by-side with DEA agents and do phone records searches for them. From the article: 'For at least six years, law enforcement officials working on a counter narcotics program have had routine access, using subpoenas, to an enormous AT&T database that contains the records of decades of Americans' phone calls — parallel to but covering a far longer time than the National Security Agency's hotly disputed collection of phone call logs.'"

T&T unit provided them with evidence that the NSA plan. Afran said he has seen the worker's log book and icipation in the project. He declined to identify the

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
> ice to give the government secret, direct access to
> ommunications 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

Posted by **Soulskill** on Saturday June 22, 2013 @08:30AM
from the points-for-consistency dept.

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

Posted by **CmdrTaco** on Wednesday May 23, 2001 @07:39PM
from the 31337-h4xx0rs-at-the-ns4 dept.

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. The
> FBI this year to allow the NSA easier access via Prism to its cloud stora
> which now has more than 250 million users worldwide. Microsoft also wo
> Intercept Unit to 'understand' potential issues with a feature in Outlook.co
> create email aliases. Skype, which was bought by Microsoft in October 2
> intelligence agencies last year to allow Prism to collect video of conversa
> Material collected through Prism is routinely 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

> oft 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
> ng laws were believed to shelter companies from being forced to modify their
> l surveillance, but experts say the Foreign Intelligence Surveillance Court may now
> erpretation. Microsoft's statement about its cooperation with NSA surveillance
> t 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
> order... These programs that violate the Bill of Rights can continue because people can't g
> 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.

OpperNerd 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

NSA Data Mining Much Larger Than Reported

Posted by **ScuttleMonkey** on Saturday December 24, 2005 @08:32PM
from the sans-surprise dept.

silassewell writes to tell us The New York Times is reporting that the

> "volume of information harvested from telecommunication data and voice networks, without approved warrants, is much larger than the White House has acknowledged."

The NSA gained the cooperation of many American telecommunication companies after 9/11 to streams of communication, both domestic and international, as a part of a presidentially approv program to hunt for

NSA Collects 200 Million Text Messages Per Day

Posted by **timothy** on Thursday January 16, 2014 @12:44PM
from the hey-why-do-you-hate-america? dept.

ilikenwf writes

obtained by Edward Snowden have revealed that the NSA collects day. These are used to gain travel plans, financial data, and social these texts and data belong to people who are not being association. Supposedly, "non-US" data is removed, but we all know ner country for analysis, which is then sent back to the NSA."

NSA Admits Searching "3 Hops" From Suspects

Posted by **timothy** on Thursday July 18, 2013 @03:44PM
from the extrapolation-nation dept.

New submitter cpitman writes

> "In a house hearing Wednesday the NSA admitted th but also perform up to a 'three hop query'. Considerin by under 6 degrees of separation, the NSA essential rights to investigate a large chunk of the world's popu 700,000 names, just how many times has Kevin Bac

Verizon Ordered To Provide All Customer Data To NSA

Posted by **samzenpus** on Wednesday June 05, 2013 @10:27PM
from the do-you-hear-what-I-hear dept.

Rick Zeman writes

d, an order by the Foreign Intelligence Surveillance Court '...requires Verizon to adata on all calls within the U.S. and between the U.S. and foreign countries on basis" for three months.' Unlike orders in years past, there's not even the of the parties needed to be in a foreign country. It is unknown (but likely) that nder the same order."

NSA Intercepted French Telephone Calls "On a Massive Scale"

Posted by **Unknown Lamer** on Monday October 21, 2013 @09:26AM
from the french-people-don't-deserve-privacy dept.

rtoz writes

> "The US National Security Agency (NSA) has been intercepting French telephone calls ' massive scale,' according to a report published in Le Monde. According to Le Monde, th recorded millions of telephone calls placed by French citizens over a 30-day period last including some placed by people with no connections to terrorist organizations. France c

NSA Tracking Cellphone Locations Worldwide

Posted by **timothy** on Thursday December 05, 2013 @07:32AM
from the relax-citizens-we're-only-watching-you-closely dept.

tramp writes

> "The National Security Agency is gathering nearly 5 billion records a day on the whereabouts of cellphones around the world, according to top-secret documents and interviews with U.S. intelligence officials, enabling the agency to track the movements of individuals — and map their relationships — in ways that would have been previously unimaginable. Of course it is 'only metadata' and absolutely not invading privacy if you ask our 'beloved' NSA."

Includes active attacks

Australian Spy Agency Seeks Permission To Hack Third-Party Computers

Posted by **Soulskill** 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 a
> inevitably, they say these changes ar

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

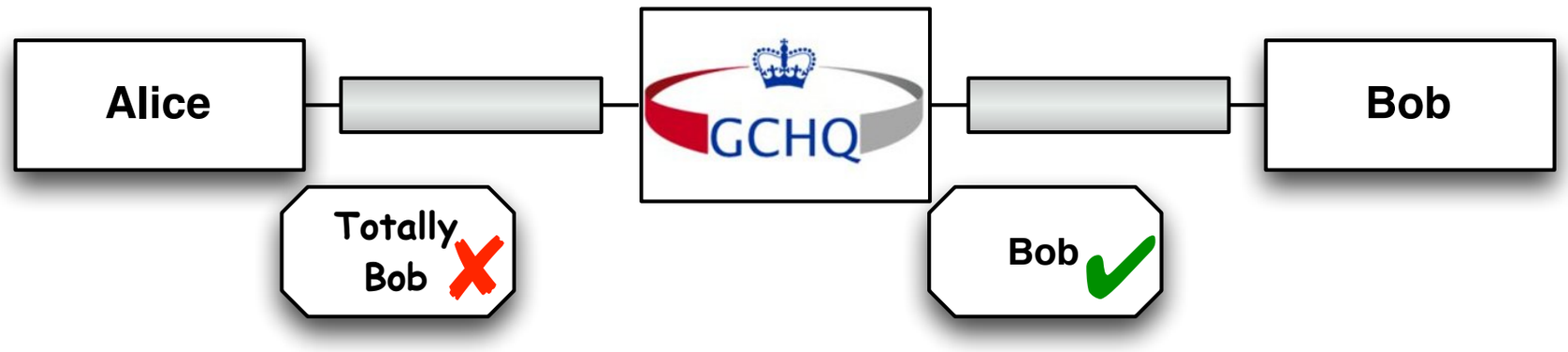
Passive attacker

- 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



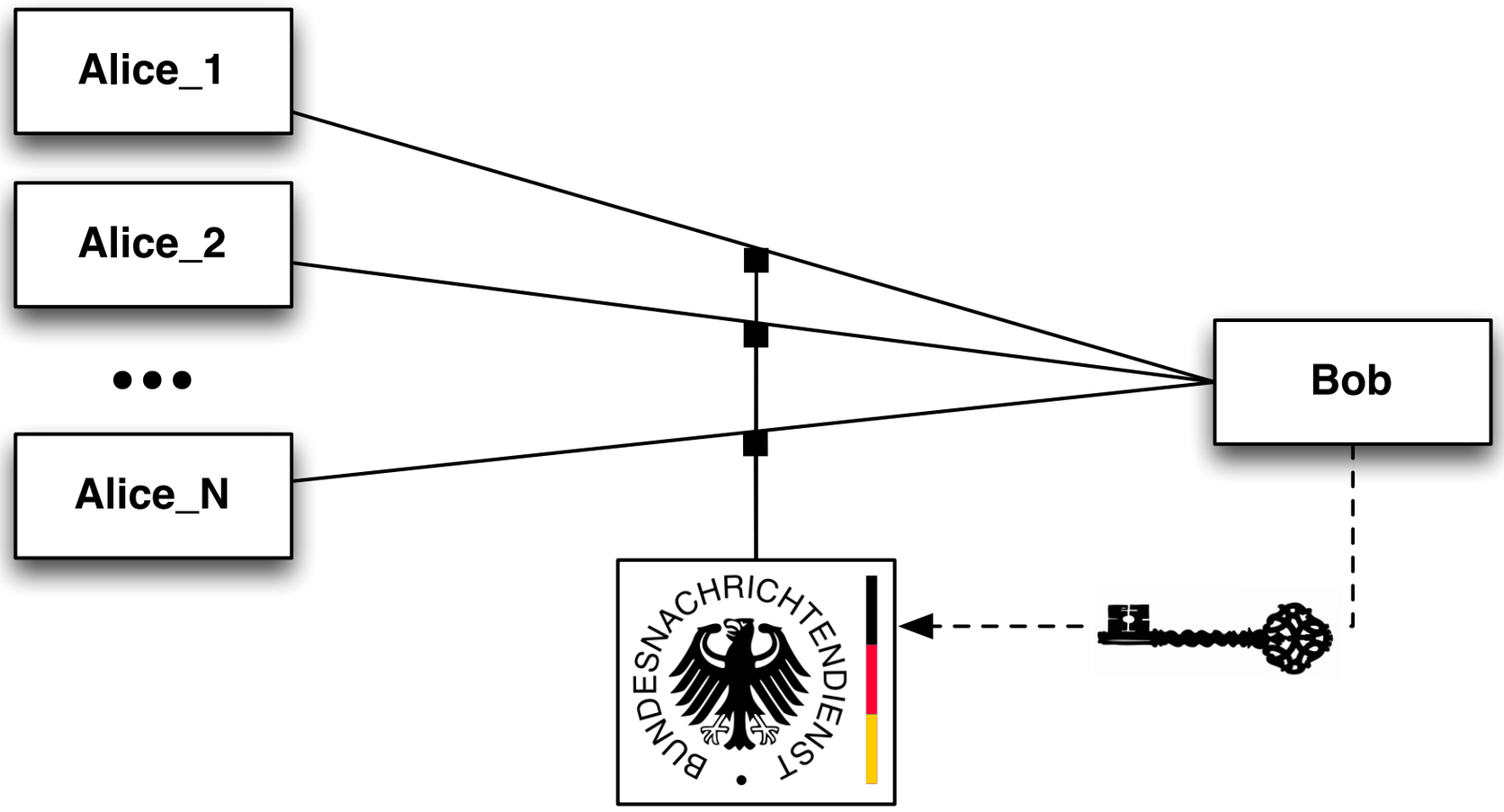
- Mitigation: Make sure you're talking to who you think you are
  - Authentication technologies (e.g., PKIX, DANE)
  - Improve information about who to trust
    - Key pinning, Certificate Transparency, DANE

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 exfilatration

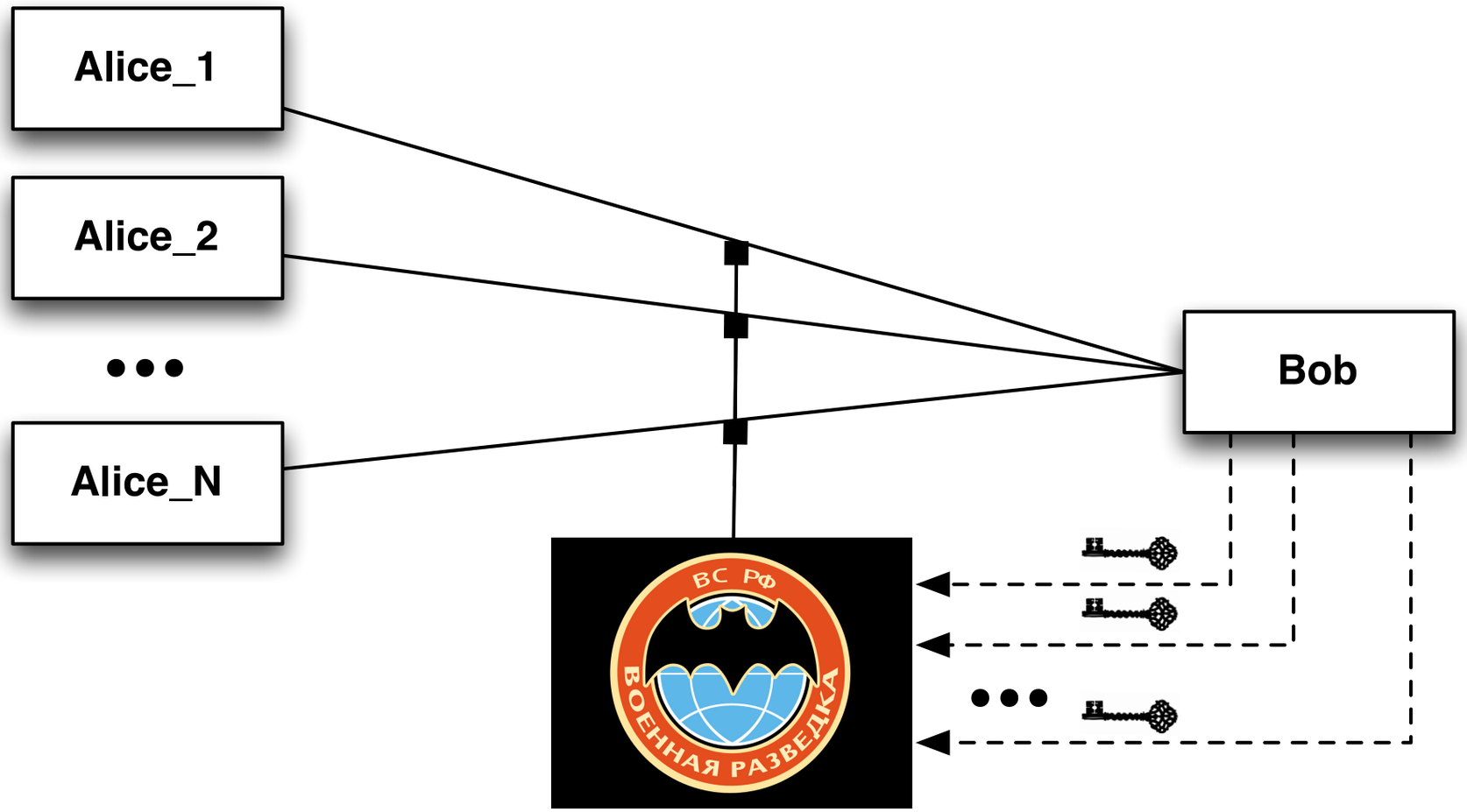
- Collaborator provides attacker with long-lived keys



- Mitigation: Use PFS to require per-session keys

Dynamic key exfilatration

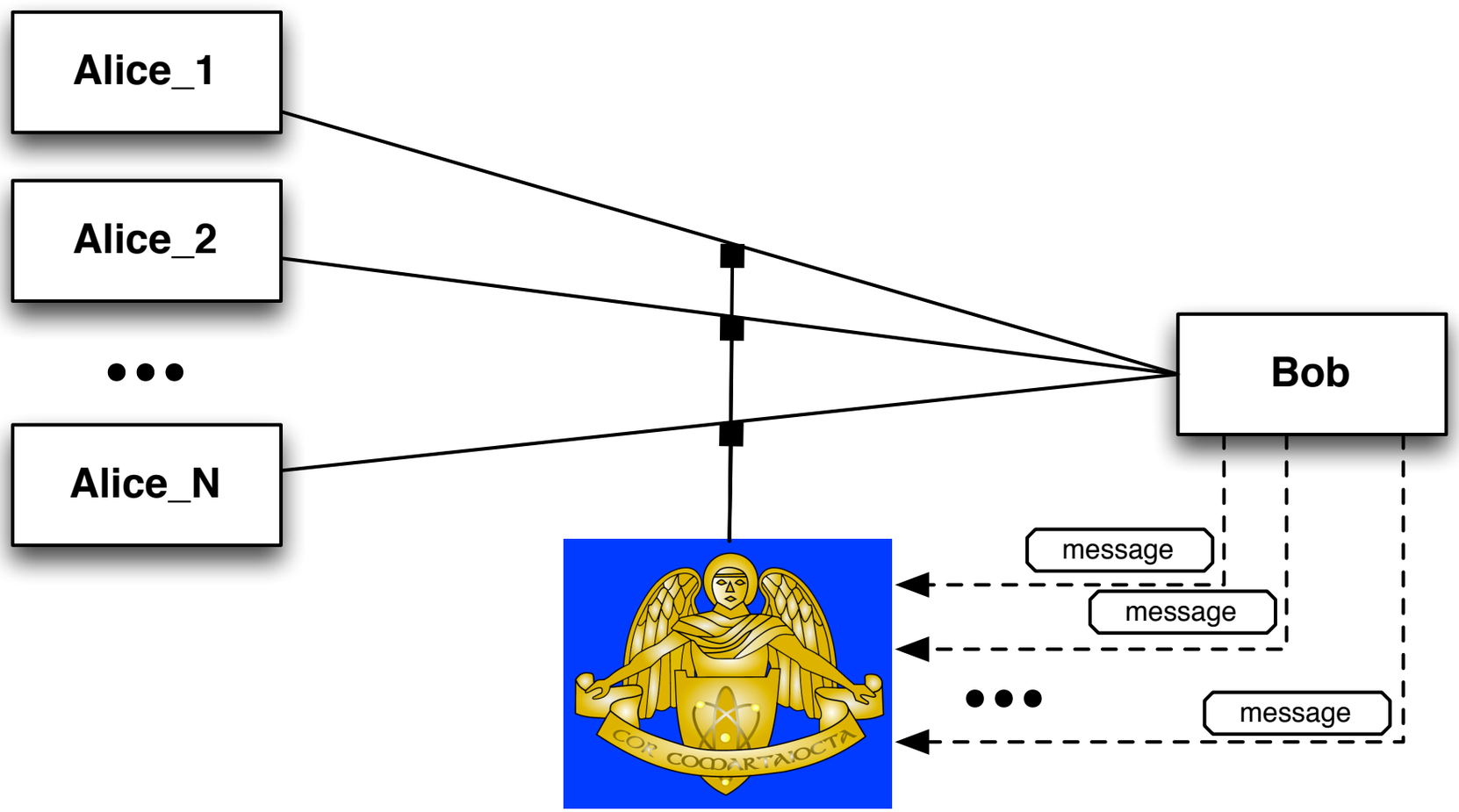
- Collaborator provides attacker with per-session keys



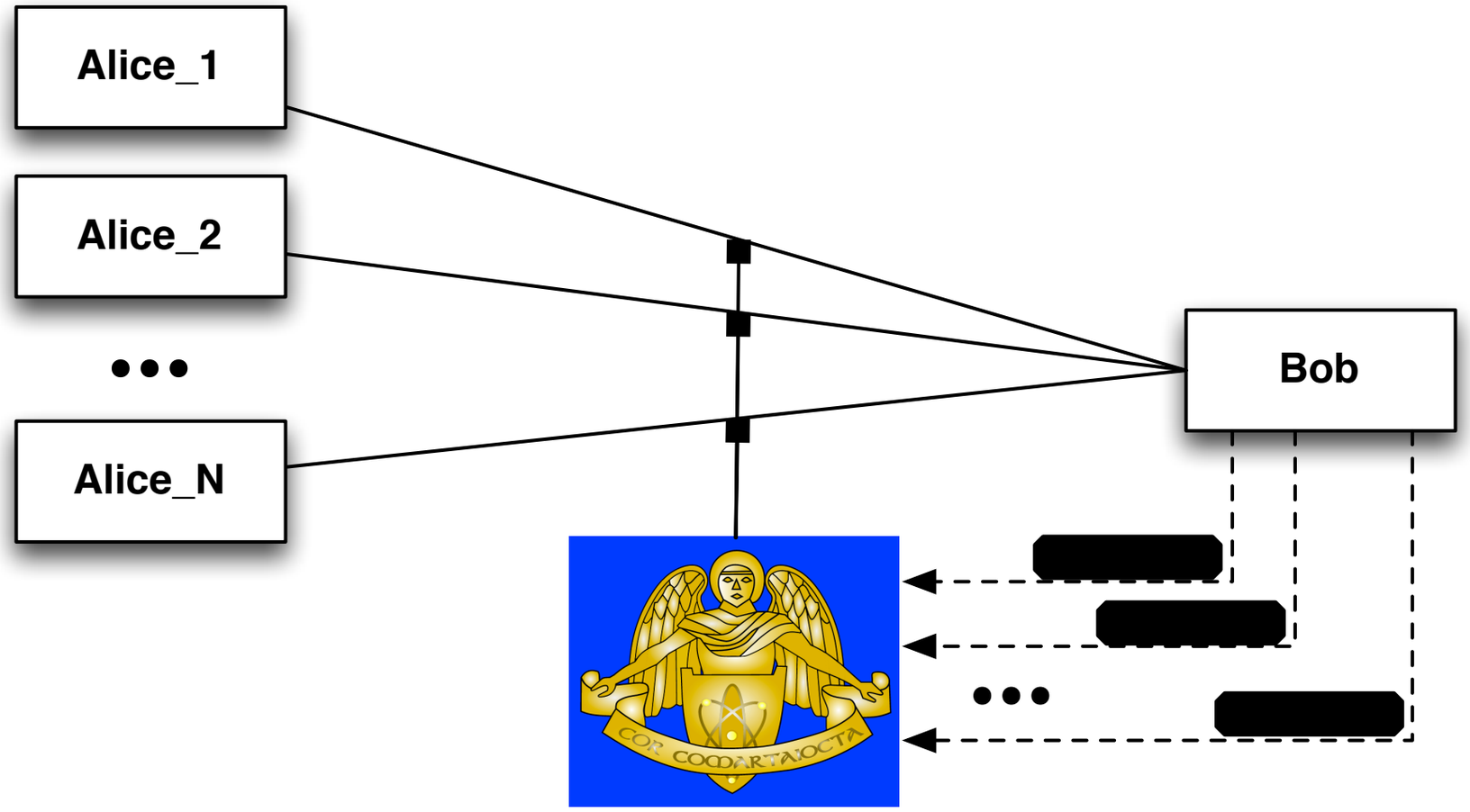
- Mitigation: Use PFS to require per-session keys

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