

Security Engineering

Ross Anderson & Yuvraj Patel*
Edinburgh University

* We will be reusing the lecture material from the previous class taught in 2022 and taught by Prof. Ross Anderson and Dr. Sam Ainsworth

What is Security Engineering?

Security engineering is about building systems to remain dependable in the face of malice, error and mischance. As a discipline, it focuses on the tools, processes and methods needed to design, implement and test complete systems, and to adapt existing systems as their environment evolves.

This course

- For Informatics students at Edinburgh – MSc / UG y4
- Lectures online for all in the world to use:
 - This introductory joint lecture on who our opponents are
 - Lectures by Prof Ross Anderson on ‘breadth’ – security policies, payment applications, psychology, economics, interaction with safety (lectures 2-6, 13)
 - Lectures by Dr Sam Ainsworth on ‘depth’ – networks, hardware, operating systems, ecosystems (lectures 7–12)
 - Concluding lectures on assurance, governance (14, 15)
 - Guest lecture (16)
- For Edinburgh students, live discussions too!
- Dr Ainsworth left the university in 2022. Yuvraj Patel will take over and cover his part in the tutorials.

Security engineering 101

- Start with a threat model. Who might attack us, why, and how? People or malware? Insiders or outsiders? Governments, crooks, or your kid sister?
- Then: security policy. What protection properties are we trying to provide? If you're trying to keep secrets, or guard money, what rules do you need?
- Then: how do you implement them? What protection mechanisms do you use, and how?
- Finally: assurance. How do you know you've done enough, and how do you convince others of that?

This lecture

- Who are the opponents?
 - State actors – Five eyes; Russia; China; others
 - Criminals – ransomware gangs, fraud gangs
 - Lawful operators – security researchers, tool vendors
 - The swamp – hate crimes, sex abuse, bullying
- What are their tools?
 - The vulnerability lifecycle
 - Zero-days and the cyber-arms market
 - Shared infrastructure – botnets, crime forums
- Further reading: Security Engineering chapter 2

3RD EDITION

SECURITY ENGINEERING

.....
**A GUIDE TO
BUILDING DEPENDABLE
DISTRIBUTED SYSTEMS**

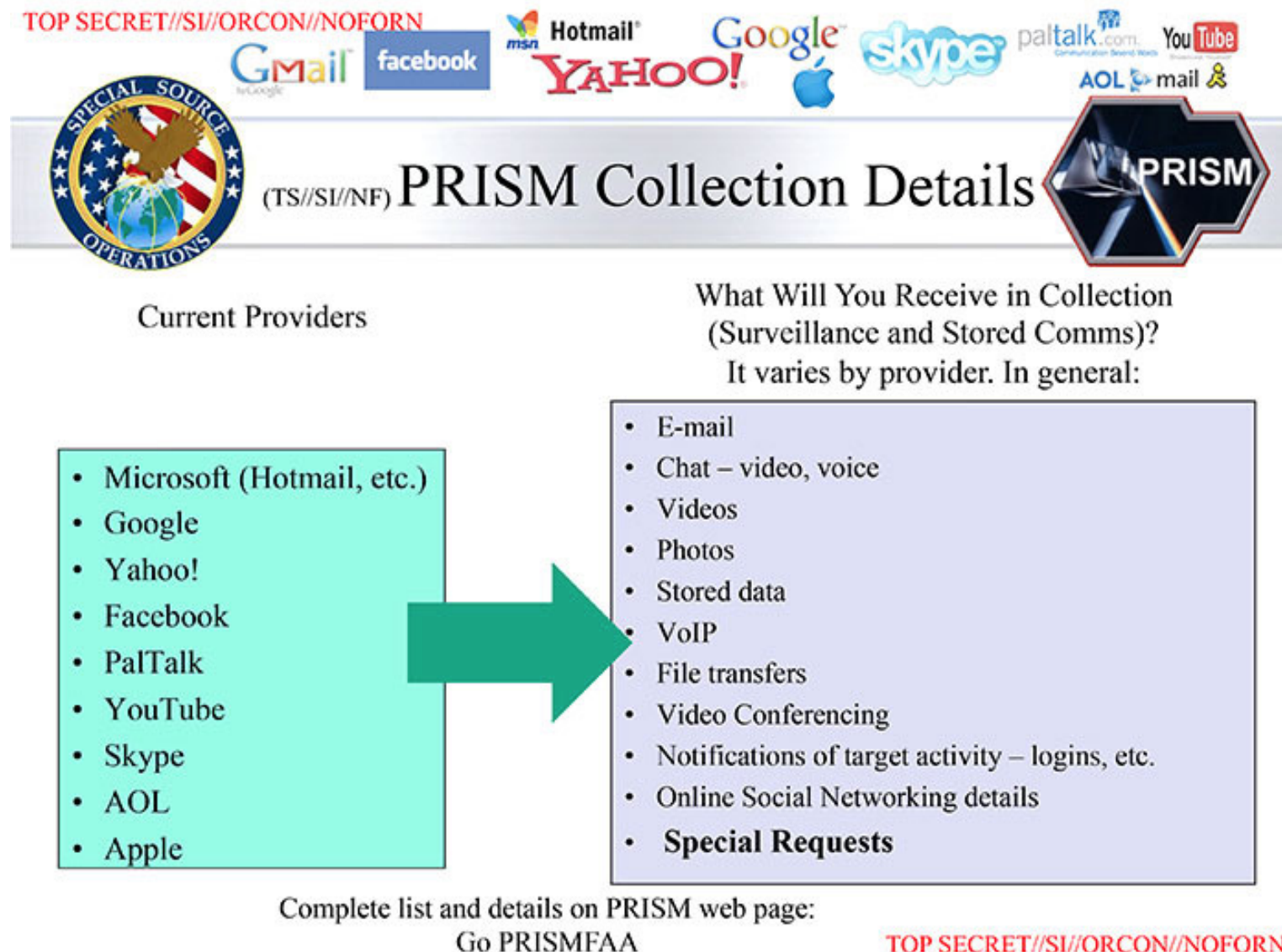
ROSS ANDERSON

.....
WILEY

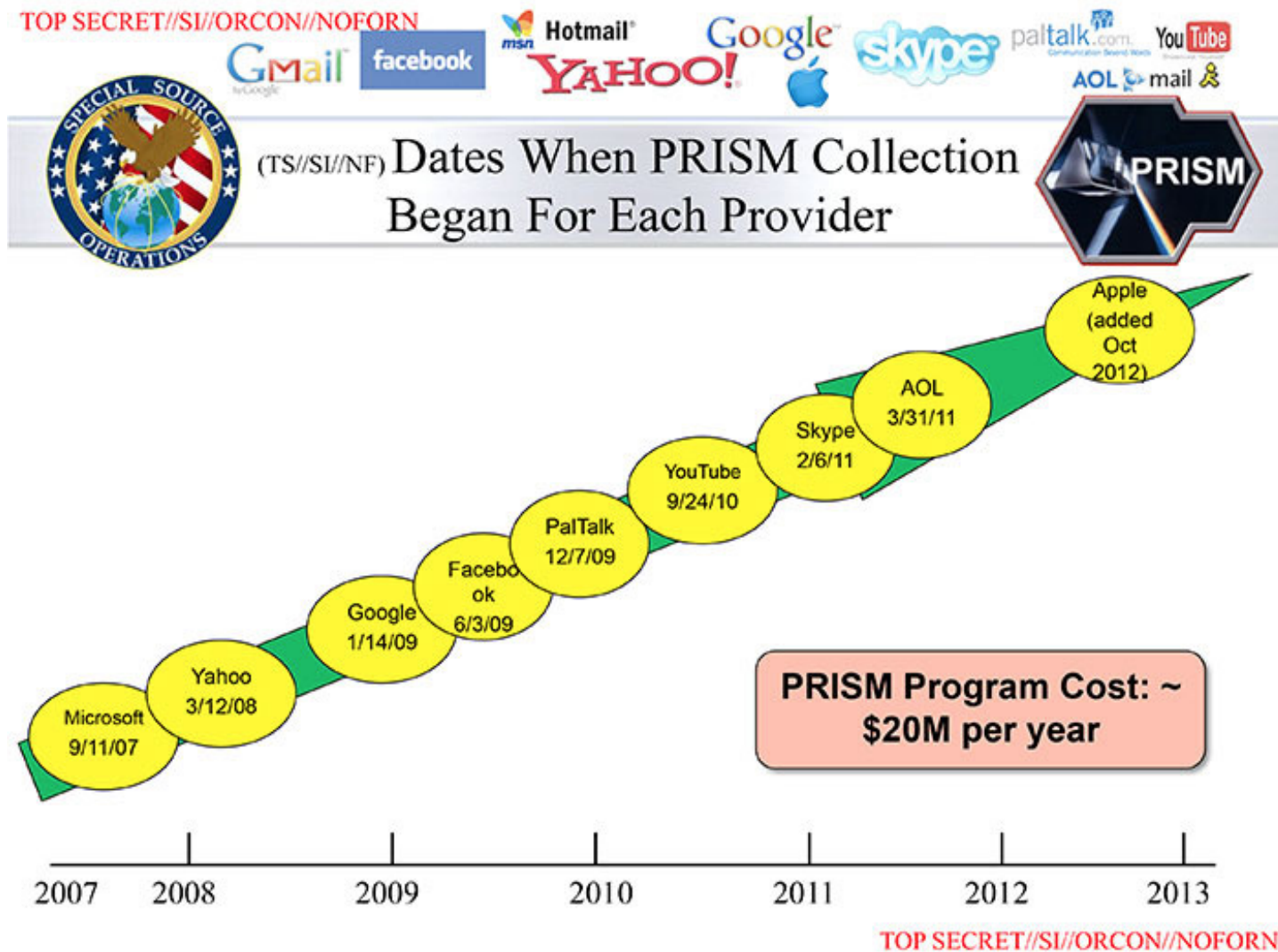
The Five Eyes

- The USA, the UK, Canada, Australia and New Zealand share intelligence infrastructure
- Many fibres follow old phone / telegraph cables; bulk wiretap in Cornwall, Gibraltar etc
- Also collect via satellite downlinks, embassies etc
- Signals intelligence agencies (NSA, GCHQ...) get way more money than traditional human spying
- The agencies sought for years to restrict / undermine cryptography ('Crypto Wars')
- 2013: Edward Snowden revealed the scale

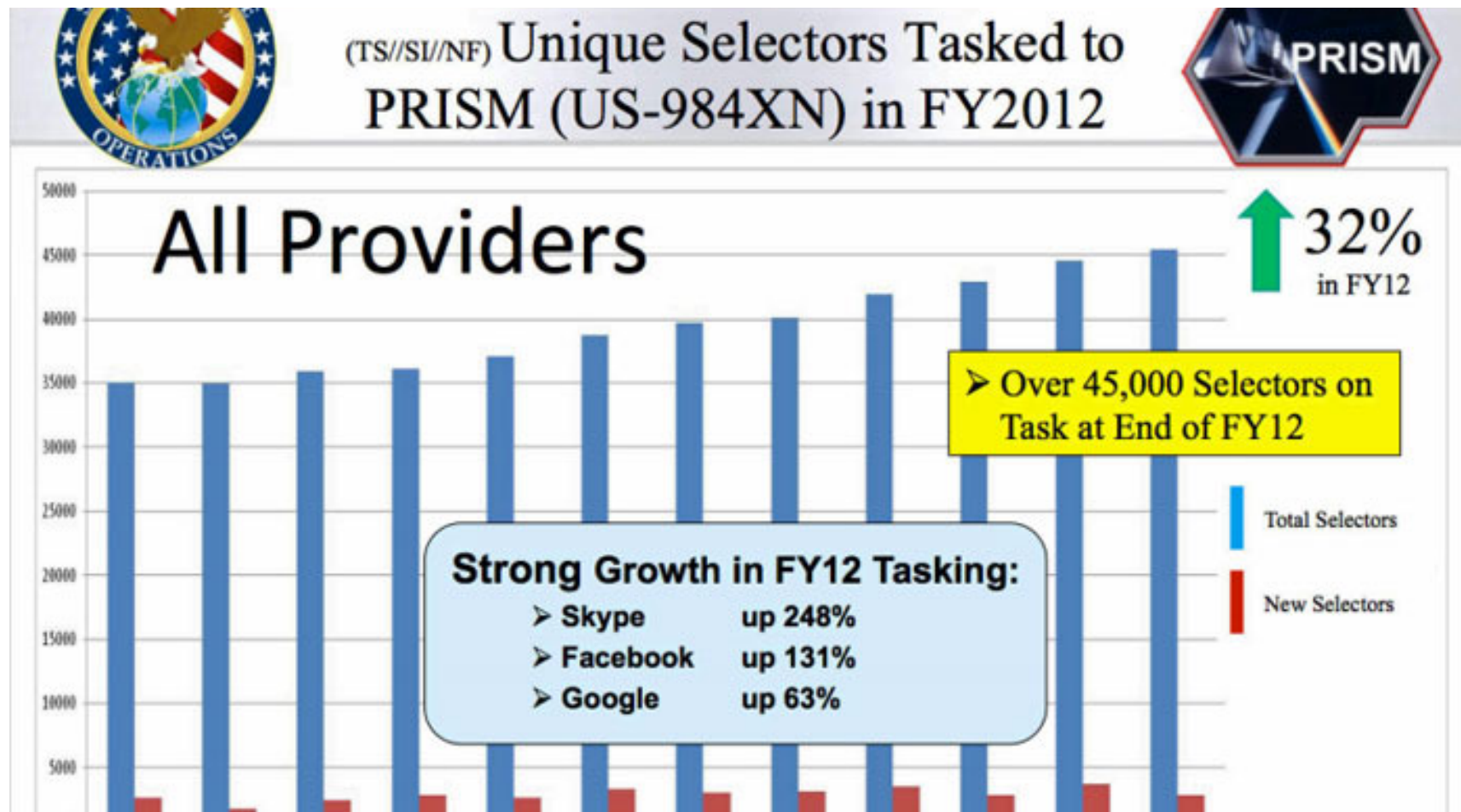
Snowden



Snowden (continued)



Snowden (continued)

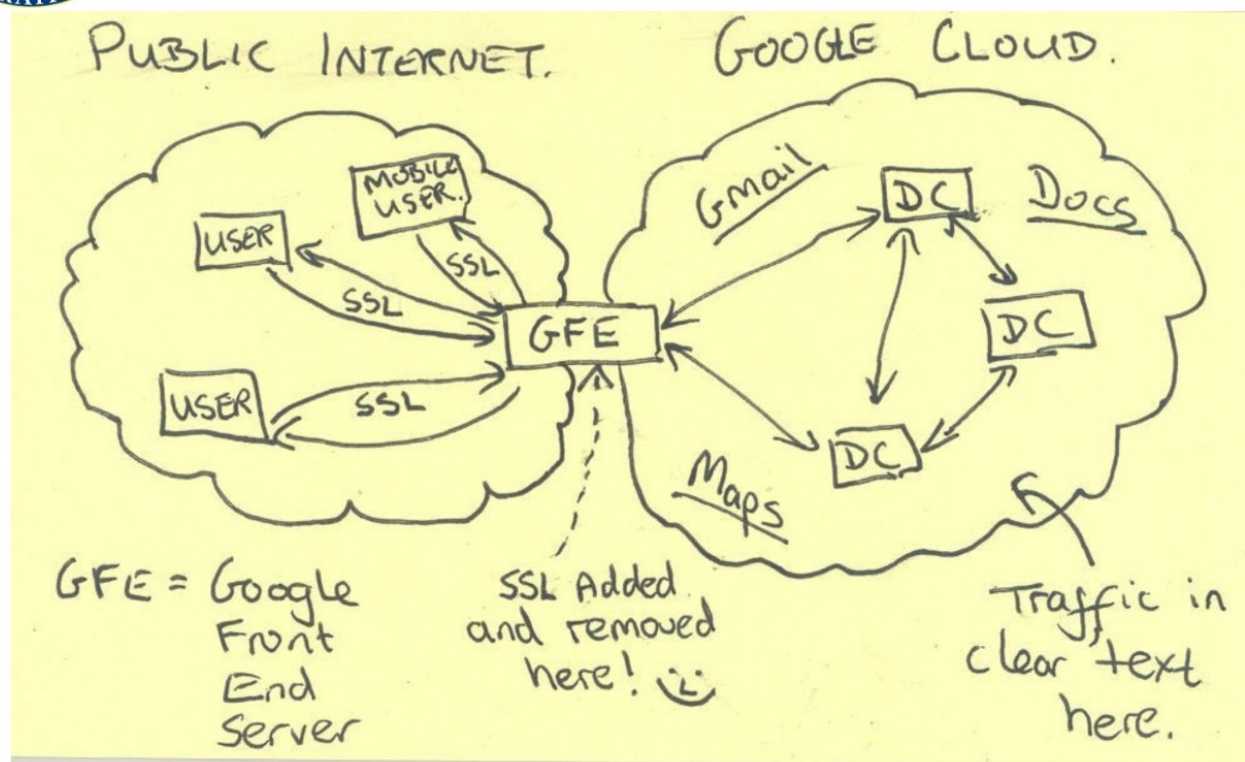


What really annoyed Google

TOP SECRET//SI//NOFORN



Current Efforts - Google



TOP SECRET//SI//NOFORN

What really annoyed the EU

- Scoping session conducted – main focus to be on enabling CNE access to **BELGACOM GRX Operator**
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles



Snowden (continued)

TOP SECRET STRAP1

Response to improving security

- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable
- Major new processing systems, SIGDEV efforts and tasking must be put in place to capitalize on this opportunity

PTD "We penetrate targets' defences."



This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221481 x30500 (non-sec) or email infoleg@gchq

© Crown Copyright. All rights reserved.

Bullrun / Edgehill

TOP SECRET//SI//TK//NOFORN

(U) COMPUTER NETWORK OPERATIONS (U) SIGINT ENABLING

This Exhibit is SECRET//NOFORN									
	FY 2011 ¹ Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 — FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding (\$M)	298.6	275.4	—	275.4	254.9	—	254.9	-20.4	-7
Civilian FTE	144	143	—	143	141	—	141	-2	-1
Civilian Positions	144	143	—	143	141	—	141	-2	-1
Military Positions	—	—	—	—	—	—	—	—	—

¹Includes enacted OCO funding. Totals may not add due to rounding.

(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this way, the SIGINT Enabling approach uses commercial technology and insight to manage the increasing cost and

The Five Eyes (summary)

- PRISM: 'most used in NSA reporting'. Such server access known as 'downstream' collection
- Warrant required: probable cause (US persons, FBI), being a foreigner (everyone else, NSA/CIA)
- TEMPORA: large-scale access to optical fibres at dozens of locations ('upstream' collection)
- Computer network exploitation (CNE): hacking, both bulk and targeted
- XKEYSCORE: a distributed search engine over more than 100 repositories of intercept worldwide

China

- America's strategic peer competitor
- Hacking went from smart people + simple tools in 2000s to more systematic operations now
- From Dalai Lama (2008) and Google (2009) to OPM (2015) to MS (2021)
- Building scale access via Belt and Road, Huawei, ZTE, TikTok,...
- Full-stack competition: chips; 'offshoring' manufacture for US firms; its own tech majors, ...

Russia, Iran, North Korea ...

- Lacking platform advantage, other countries rely on spear-phishing and hacking
- Iran's uranium enrichment centrifuges hacked by US and Israel 2008–9 (Iran retaliated against Saudi)
- North Korea hacked Sony Pictures in 2014
- Russia uses cyber weapons in regional conflicts, e.g. Ukraine's grid in 2015, NotPetya in 2017
- SolarWinds hack against US gov, companies
- Also tried to influence the 2016 US election, from hacking DNC to troll farms supporting Trump

Intelligence doctrine

- According to NSA's former scholar-in-residence Joshua Rovner, intelligence contests are five things:
 - Race between adversaries to collect more / better information
 - Race to exploit this to improve one's position
 - Reciprocal effort to undermine adversary morale, institutions and alliances
 - Contest to disable capabilities through sabotage
 - Campaign to preposition assets for the event of conflict
- They are never really won or lost...

Cybercrime

- In 2019, the UK suffered just over 1m legacy property crimes like burglary and car theft
- Yet about 2.5m frauds and scams, mostly online
- We'll discuss payment fraud in lectures 2, 3, 5
- There's a whole ecosystem of bulk attackers, targeted attackers, tool providers, cashout gangs...
- Criminal infrastructure includes unregulated cryptocurrency exchanges and botnets (more later)
- Big growth area since 2020: ransomware

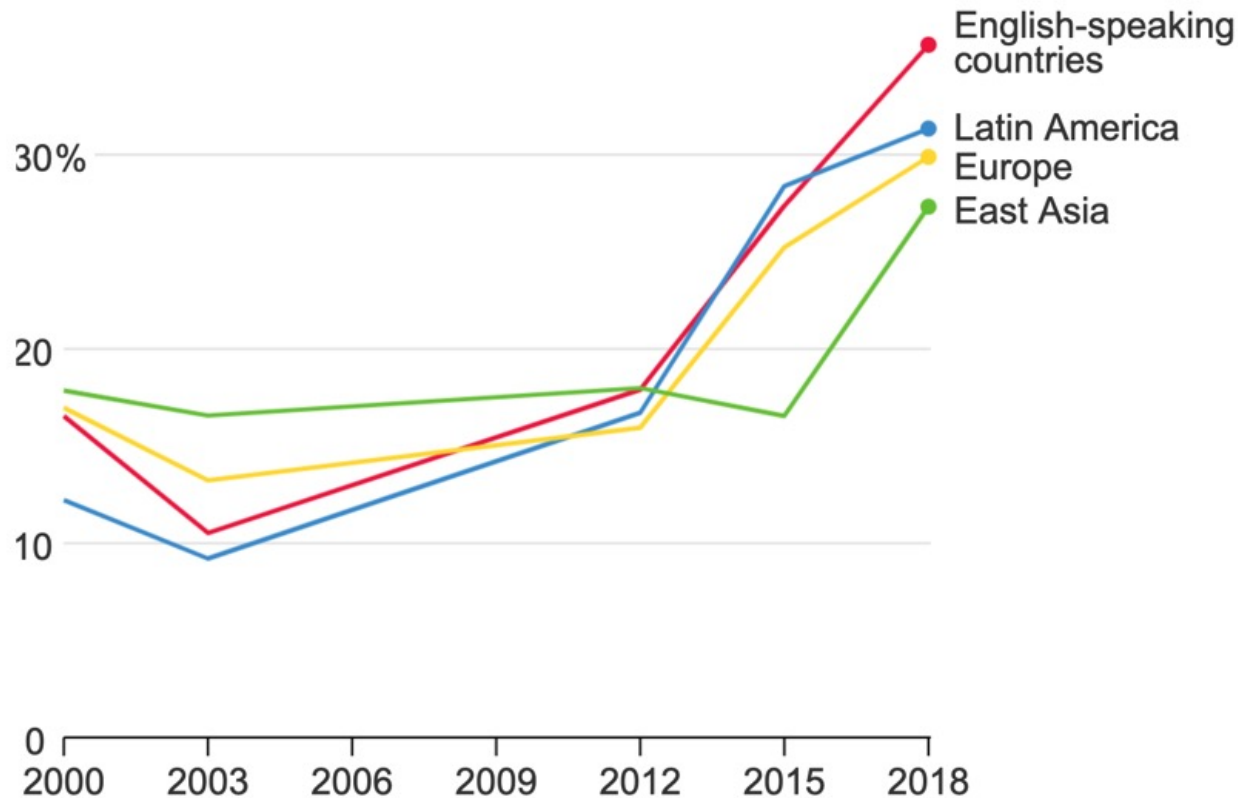
Abuse

- Terrorism recruitment and child sex abuse material
- Hate campaigns such as Gamergate
- Intimate relationship abuse
- School and workplace bullying
- Growing pressure from governments to censor
- Big service firms already do a lot of filtering at great expense (sex abuse, terror, hate speech, nudity)
- 'Like' and 'Retweet' led to performative shaming; social media became an outrage machine

Social media and mental health?

Lonely at School

The share of students reporting high levels of loneliness at school has increased sharply since the early 2010s.



Who is the Opponent?

Tools, Zero-days, and Attacks on Systems

The Kill Chain: Stuxnet (2008)

- Used by the US to target Iranian Nuclear programme, then escaped...
- 7 Zero days (undisclosed vulnerabilities in the wild): four in Windows, three in Siemens Programmable Logic Controllers
- Chain started with a USB drive being plugged in!
- Complicated, blurred chain of social engineering, zero days, and old but unpatched software.

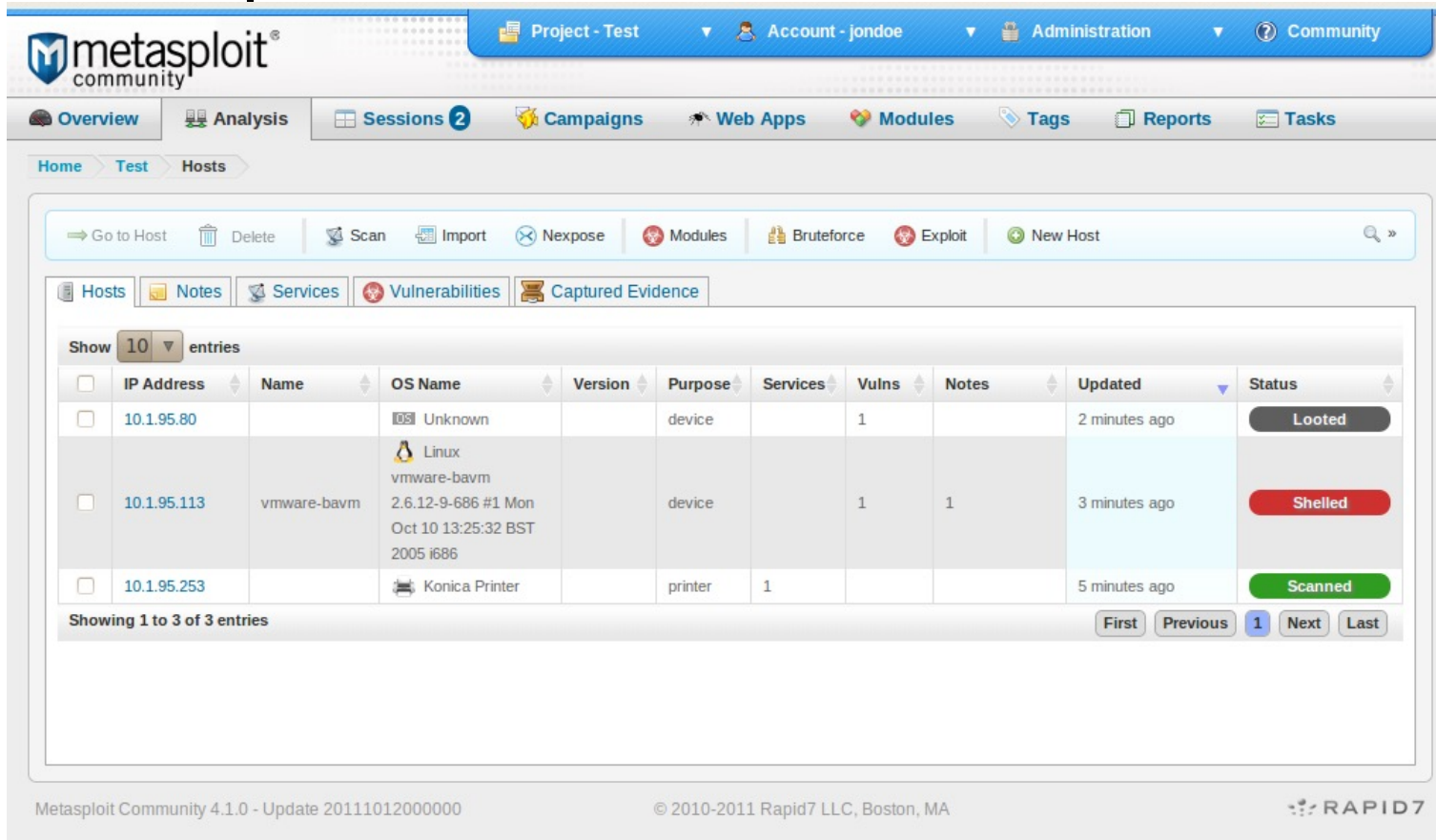
Who is the opponent (5)? Security Researchers

- Many of the initial tools of attack look an awful lot like tools of defence: fuzzers, debuggers, sanitizers
- “Good Geeks” responsibly disclose vulnerabilities before they are widely exploited
- “Bad Geeks” sell to nation states for \$\$\$
- iDefense (early 2000s): geeks will take tiny valuations in order to not get sued!
- Clever companies don’t threaten to sue researchers, and instead have a bug bounty programme.
- More in Security Economics (Lecture 5?)

From Vulnerability to Exploit

- So you have your bug in a program (e.g. a buffer overflow, a use-after-free, type confusion). How do you turn that into a useable attack?
- You can't just store some code in a data buffer and execute it any more...
- Address-Space Layout Randomisation (ASLR) and Data Execution Prevention get in your way

From Vulnerability to Exploit: Metasploit

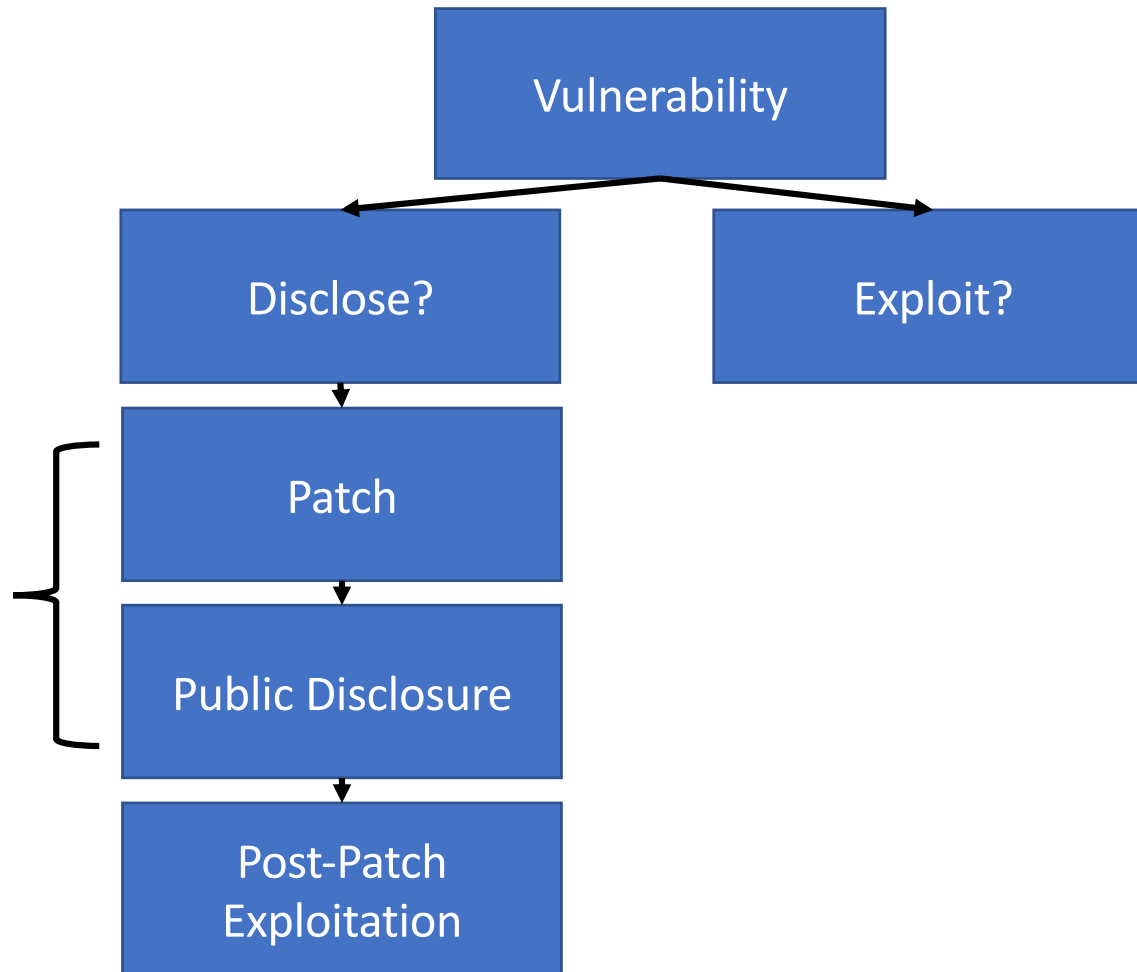


The screenshot displays the Metasploit Community web interface. The top navigation bar includes links for Project - Test, Account - jondoe, Administration, and Community. Below this, a secondary navigation bar features Overview, Analysis, Sessions (2), Campaigns, Web Apps, Modules, Tags, Reports, and Tasks. The main content area is titled 'Home > Test > Hosts' and contains a toolbar with actions like Go to Host, Delete, Scan, Import, Nexpose, Modules, Bruteforce, Exploit, and New Host. A tabbed interface shows Hosts, Notes, Services, Vulnerabilities, and Captured Evidence. The Hosts tab is active, displaying a table with 10 entries. The table columns are IP Address, Name, OS Name, Version, Purpose, Services, Vulns, Notes, Updated, and Status. Three entries are visible: 10.1.95.80 (Looted), 10.1.95.113 (Shelled), and 10.1.95.253 (Scanned). The footer shows 'Metasploit Community 4.1.0 - Update 20111012000000', '© 2010-2011 Rapid7 LLC, Boston, MA', and the 'RAPID7' logo.

IP Address	Name	OS Name	Version	Purpose	Services	Vulns	Notes	Updated	Status
10.1.95.80		Unknown		device		1		2 minutes ago	Looted
10.1.95.113	vmware-bavm	Linux vmware-bavm 2.6.12-9-686 #1 Mon Oct 10 13:25:32 BST 2005 i686		device		1	1	3 minutes ago	Shelled
10.1.95.253		Konica Printer		printer	1			5 minutes ago	Scanned

By Self created session - Metasploit Community
Edition, CC BY-SA 3.0,
<https://en.wikipedia.org/w/index.php?curid=33606448>

The Vulnerability Lifecycle



Responsible Disclosure

- Google Zero: “***Disclosure deadline of 90 days. If an issue remains unpatched after 90 days, technical details are published immediately. If the issue is fixed within 90 days, technical details are published 30 days after the fix.***”

<https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html>

Responsible Disclosure: CERT

- CERT vulnerability reporting chain: JANET CSIRT – UK NCSC – Pittsburgh US NSA – Microsoft's Patch Tuesday.
- 45+/90 day window of disclosure.
- Liability shield/credit for the hacker.
- Only good for OS/networks, not finance.

https://www.ncsc.gov.uk/files/NCSC_Vulnerability_Toolkit.pdf

<https://vuls.cert.org/confluence/pages/viewpage.action?pageId=4718642>

<https://hackerone.com/disclosure-assistance>

Google on Heartbleed



"With early access to the patch... Google **infrastructure teams had already quietly patched** a small number of key externally facing systems... However, no other internal teams knew about the issue.

Once the bug became publicly known, exploits were developed quickly in frameworks such as Metasploit. Facing an accelerated timeline, many more Google teams now needed to patch their systems in a hurry.

Google's security team used **automated scanning to uncover additional vulnerable systems**, and notified affected teams with instructions to patch and to track their progress. The memory disclosure meant that **private keys could be leaked**, which meant that a number of services needed **key rotation**."

Building Secure & Reliable Systems, Chapter 7, on the OpenSSL Heartbleed bug

Kernel Page-Table Isolation

Signed-off-by: Dave Hansen <dave.hansen@linux.intel.com>

Cc: Moritz Lipp <moritz.lipp@iaik.tugraz.at>

Cc: Daniel Gruss <daniel.gruss@iaik.tugraz.at>

Cc: Michael Schwarz <michael.schwarz@iaik.tugraz.at>

...

Page Table Isolation (pti, previously known as KAISER[1]) is a countermeasure against attacks on kernel address information.

There are at least three existing, published, approaches using the shared user/kernel mapping and hardware features to defeat KASLR

...

This approach helps to ensure **that side-channel attacks that leverage the paging structures do not function when PTI is enabled.**

Really? It just stops leaking of
Kernel structure locations does it?
At 30% worst-case slowdown?

<https://lkml.org/lkml/2017/12/18/1523>



Meltdown

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

Who reported Meltdown?

Meltdown was independently discovered and reported by three teams:

- [Jann Horn](#) ([Google Project Zero](#)),
- [Werner Haas, Thomas Prescher](#) ([Cyberus Technology](#)),
- [Daniel Gruss, Moritz Lipp, Stefan Mangard, Michael Schwarz](#) ([Graz University of Technology](#))

Is there a workaround/fix?

There are patches against Meltdown for Linux ([KPTI \(formerly KAISER\)](#)), Windows, and OS X.

<https://meltdownattack.com/> published **2018/01/03**

Coordinated Disclosure

- When multiple parties are vulnerable, responsible disclosure becomes coordinated disclosure
- How do you keep all of the parties honest?
- How do you stop one patch from betraying the existence of vulnerabilities in other products?
- Public Relations can often be as critical as the fix itself...

Don't obsess over the Zero Day!

- Old devices: the Android ecosystem is a mess, and lots of people just don't patch!
- If you need to patch a reliable system, will it break?
- Google SRS: *"Before you tackle a same-day zero-day vulnerability response, make sure you're patched for the 'top hits' to cover critical vulnerabilities from recent years."*
- Bugs in your own public-facing code: XSS, SQL Injection still big hitters

What's wrong with this?



<https://www.zdnet.com/article/java-updater-dumps-ask-toolbar-adware-replaces-it-with-yahoo-search/>

Hierarchy of Tools: the Swamp

- Not everybody is using sophisticated zero days...
- App store spyware for e.g. partner abuse.
- Crime tools: Remote Access Trojans (RATs), ransomware
- DDoS for hire
- States still use crimeware! Don't use state-of-the-art if you can hide in plain sight with standard malware.
- Lines also get blurred with criminals getting hold of nation-state attacks, e.g. 2017 NSA Leak

“But Sam, I don’t need to worry about security! My app isn’t storing anything secret”



<https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>
<https://twitter.com/Nrg8000/status/957318498102865920>

Summary

- The most sophisticated attacks combine social engineering with zero days to get around working aspects of security policies.
- It's not *just* the user that's to blame, but you must design for users.
- It's YOUR job to build systems that work in the face of user exploit, against the right kind of attacks/attackers.

Note: Your first tutorial is next week on 25th January from 4:10 PM to 6 PM. Please do attend the tutorial class. We will be releasing the questions on 25th January that we will cover in the tutorial.