THE UNIVERSITY of EDINBURGH
informatics

SCHOOL OF INFORMATICS

PHD FAIR

Thursday 12 November 2026

Meet us at the Informatics Forum, 10 Crichton Street, Edinburgh, EH8 9AB

From 13.00 to 16.00

Contact: igs@inf.ed.ac.uk



THE UNIVERSITY of EDINBURGH

EDINBURGH
extraordinary futures await

Security Engineering

INFR11208 (UG4) // INFR11228 (MSc)



Daniel W. Woods
Email: daniel.woods@ed.ac.uk

Parallels between Network and Banking Security

1. **Money Creation**

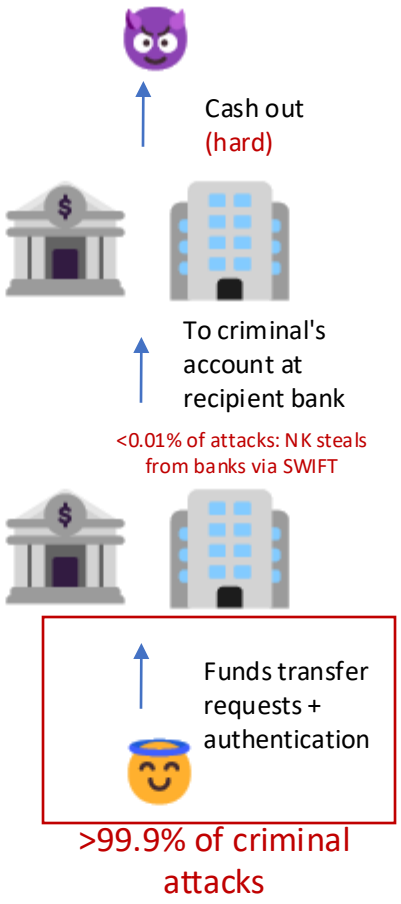
   Violate Clark-Wilson integrity model and credit criminal's account without debiting another account
   - Hard thanks to MAC
   - No known examples, which would exploit implementation details
     - Lucky given this violates trust in the entire banking system

2. **Break authentication and impersonate the victim**

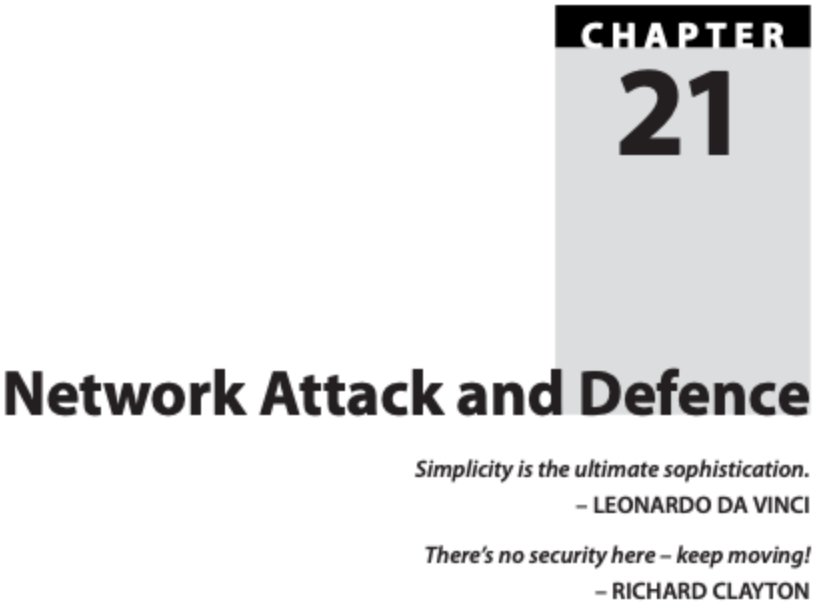
   Work within Clark-Wilson model and credit criminal's account by debiting victim's account via the criminal authenticating as the victim (or some delegated authority)
   - All kinds of attacks have been demonstrated here
     - Forging signature of a physical cheque
     - Getting access to victim's banking website account/app
     - Impersonating card, stealing/bypassing PIN, manipulating terminal
     - Compromise SWIFT to manipulate interbank transfers
   - Occasionally used by cyber criminals at scale

3. **Socially engineer the victim**

   Work within Clark-Wilson model and socially engineer victim to credit criminal's account by debiting their own account, authenticating as themselves
   - Vast majority of cybercrime losses across investment fraud, business email compromise etc



Chapter 21: Network Attack and Defence



https://www.cl.cam.ac.uk/archive/rja14/Papers/SEv3-ch21.pdf

Early Network Sec

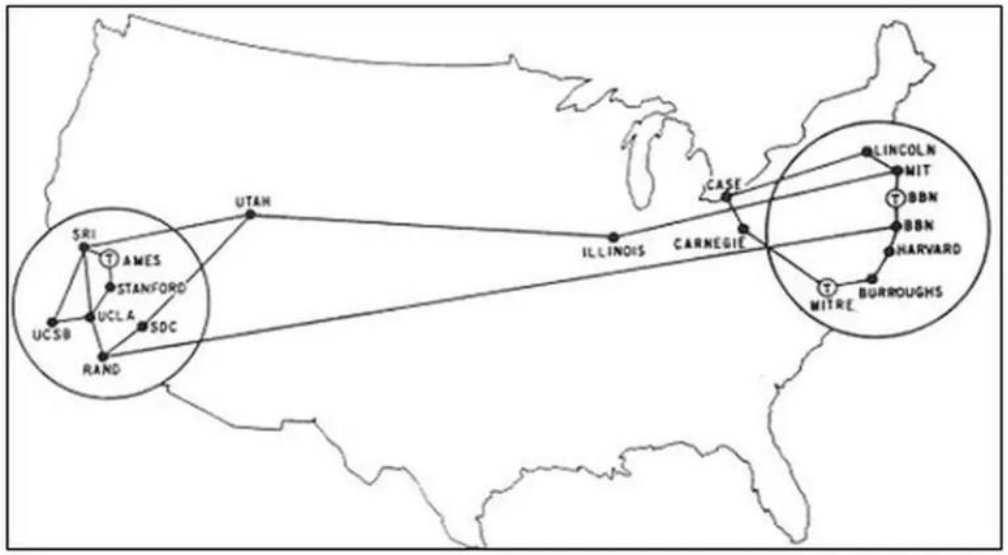
Security Engineering in 1970s

- Threat model
  - Researchers sharing research
  - Outages the main problem
- Security mechanisms
  - Design open systems with fault tolerance in mind
  - Security is useless overhead
  - Punish "bad" users

What changed and when?

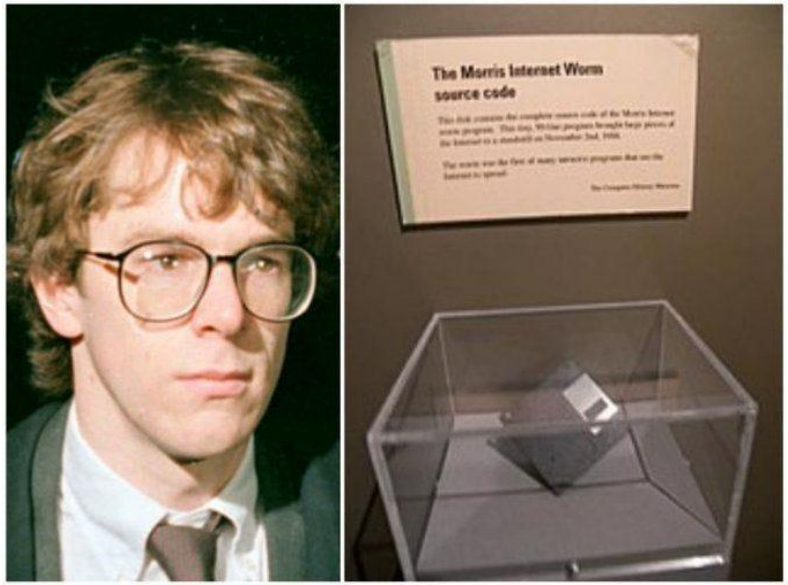
- Morris worm 1988
- ISPs connecting the public
- Ecommerce in 1990s

[Good history podcast]



By 1971, Arpanet connected the east and west coasts of the US, but did not go beyond

https://www.bbc.co.uk/news/technology-35579225



Denial of Service

Threat model

- 1990s: Asymmetric protocol design
  - Panix SYN flood: Recipient reserves chunk of memory for each request
  - Reflector attacks prevent blocking
    - ISPs inconsistent on fix (BCP38)
    - Weakest link/externality problem
  - Some protocols amplify volume
    - NTP (2010s), memached etc
- 2000s: Botnet of many PCs, later IoT devices
- **What changed and when?**
- Threat landscape:
  - no trust in extortionists, later arrested
  - Criminals use machines more profitably
- Cloud computing mostly solves DDoS
  - Professional hosting
  - CDNs, load balancing etc
  - ...but Mirai attack on DNS provider 2016
- DDoS a problem for gamers and journalists



Technology | CYBERTIMES

The New York Times ON THE WEB

September 14, 1996

New York's Panix Service Is Crippled by Hacker Attack

By ROBERT E. CALEM

'Mafiaboy' charged with cyber-terrorism

AP in Montreal

Thu 20 Apr 2000 01.06 BST

Michael Calce, infected 200 devices at three separate university networks. He then coordinated the machines to flood Internet giants like Yahoo, Amazon and eBay with traffic, knocking them offline for hours

Russian bookmaker hackers jailed for eight years

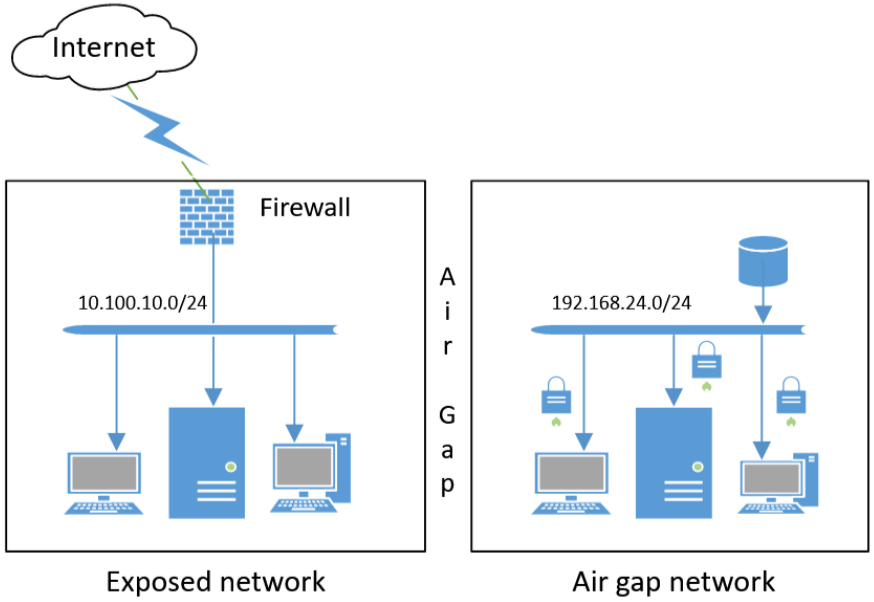
05 Oct 2006, 8:06 am

Three Russian hackers convicted of running denial of service attacks against UK bookies have each been sentenced to eight years imprisonment and fined $3,700.

Securing the perimeter

Controlling remote access

1990s: Perimeter Security





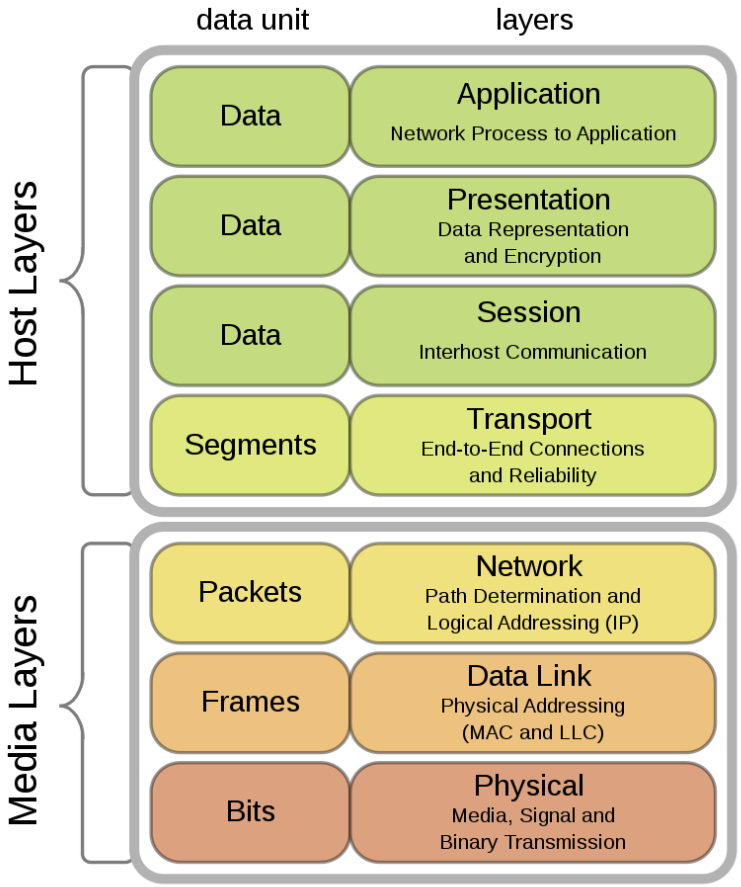
- Threat model
  - All threat actors are outside the network

Where does this work? Why does it fail?

Filtering: Firewalls

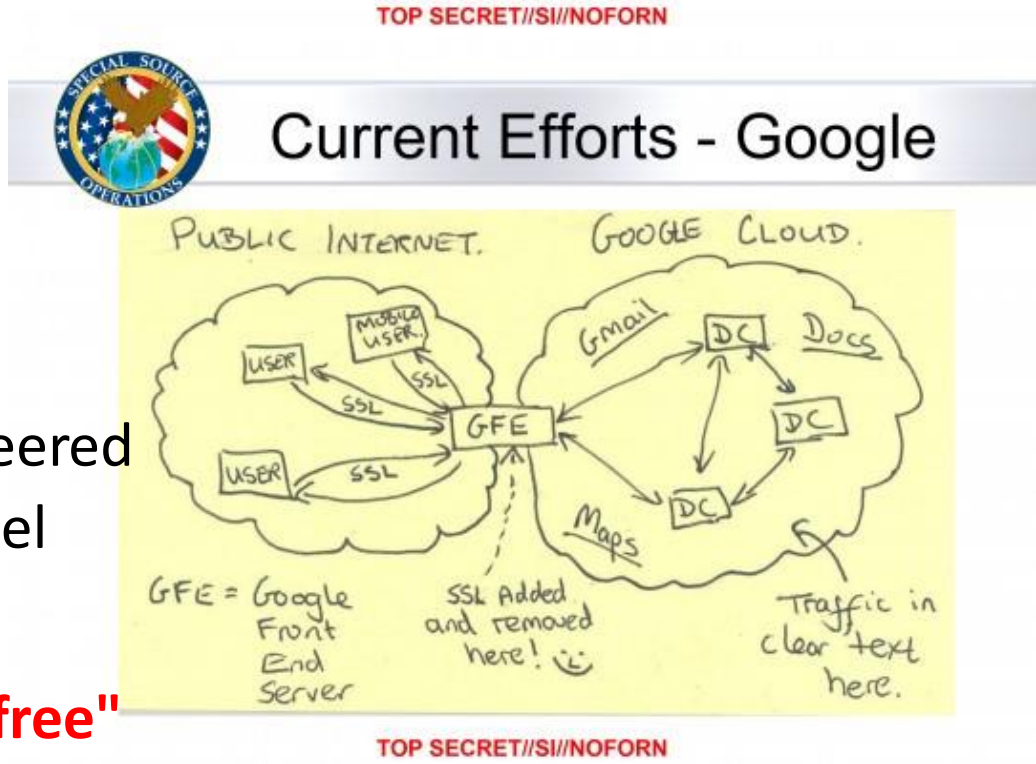
- Filtering at many levels
  - Block malicious IPs and ports
  - Circuit gateways – intermediate TCP sessions
  - Deep packet inspection at app layer
- DLP solutions
  - Terminate sessions if too much traffic flows

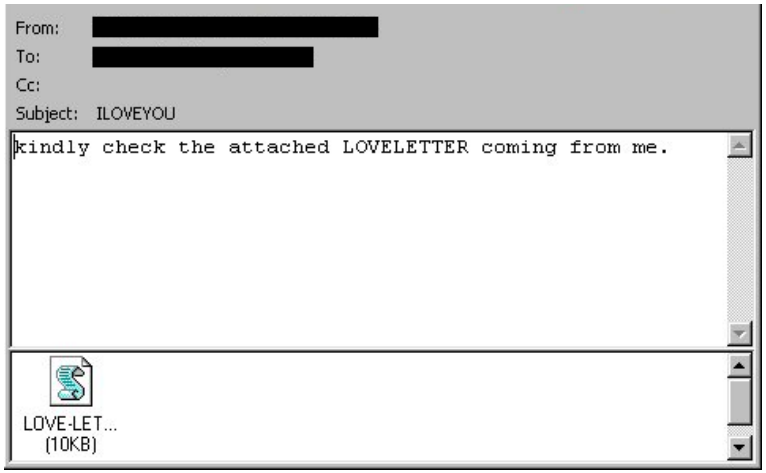
What goes wrong?



Where perimeters fail

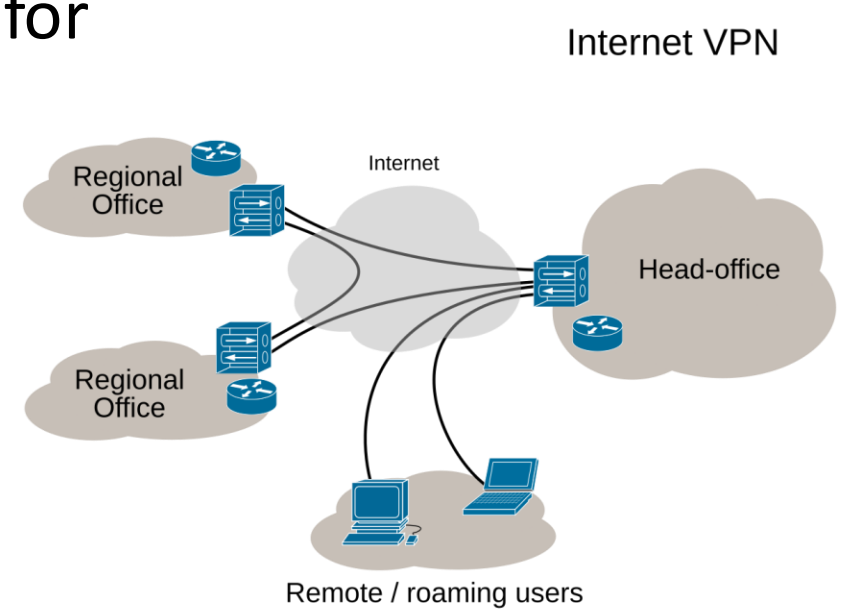
- Untrustworthy insiders
  - Malicious or socially engineered
  - A problem for any sec model
- **Web + email**
  - **"Information wants to be free"**
- **Remote work**
- A sufficiently large org
- "Sophisticated" attackers
  - See NSA





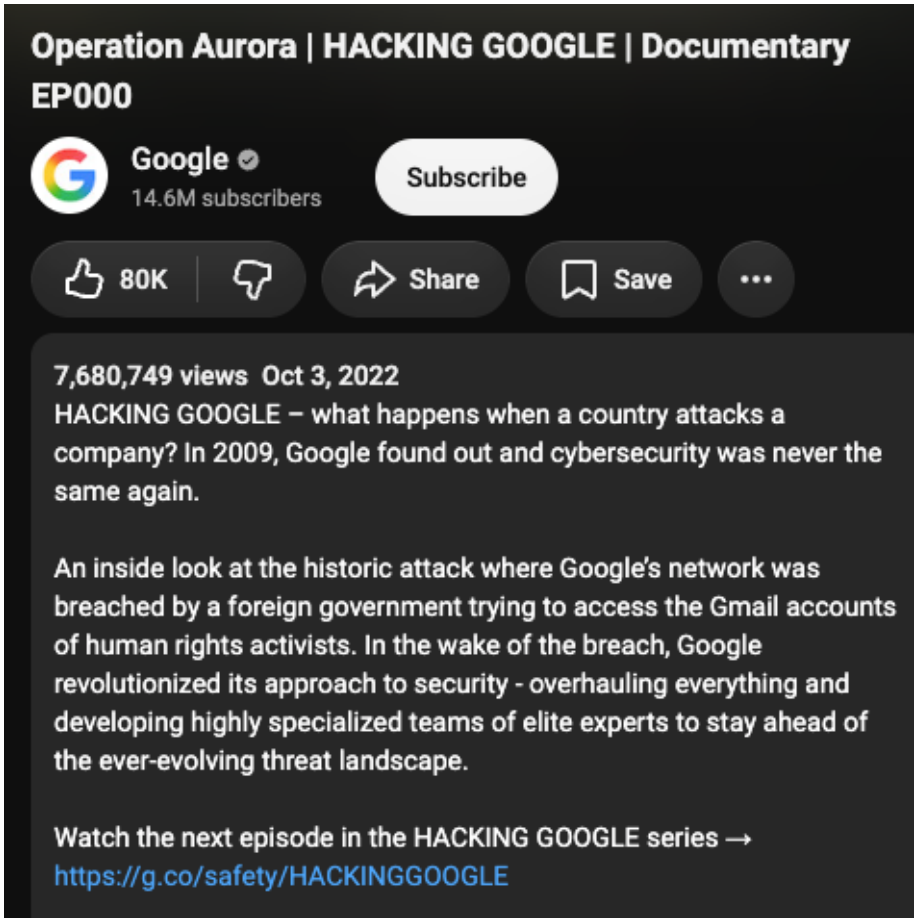
Remote work and VPNs

- **Idea:** Bypass network controls for authorised users/networks
- **What went wrong:**
  You can't put the VPN behind a VPN
  - Exploits
  - Stolen creds
  - MFA bypass
- VPN the leading initial access vector in modern incidents
  - Sophos, Coalition, Arctic Wolf



The birth of Zero Trust

- 2009 state actor from China spear phishes employees and pivots internally
  - Accesses source code
  - Accesses gmail accounts of human rights activists
- Google launches BeyondCorp
  - And markets the idea!!
- Nation state actor capabilities in 2009 reach criminals in....?



https://www.youtube.com/watch?v=przDcQe6n5o

"Full" deperimeterisation (Zero trust)

- **Idea:** Enforce access control at service/data level
  - Customer DB
  - SaaS apps
  - Web apps
  - BYOD/mobile
  - Cloud
- **What goes wrong:**
  Time cost of constant auth
- **Modern approach**
  - Contextual auth
    - More auth for more sensitive data
  - Trust signals
    - Use device of login
    - Phishing resistant MFA
    - Monitor behaviour
    - Biometric auth
    - …

What goes wrong

Breaking Into Your Network? Zer0 Effort. - DEF CON 33 Overview

Gavin Holt | 09 August 2025

Introduction

At DEF CON 33, AmberWolf presented the results of a research campaign investigating the security of Zero Trust Network Access solutions (specifically Zscaler, NetSkope and Check Point Harmony SASE). **Our research uncovered critical flaws in these market leading solutions, allowing attackers to escalate privileges on end user devices and to completely bypass authentication, granting access internal resources as any user!**

Ransomware Actors Show Up In Person to Steal Law Firm Data

The FBI warned that the extortion gang Silent Ransom Group is targeting law firms and social-engineering its way into servers and databases.

Alexander Culafi, Senior News Writer, Dark Reading
May 27, 2026

4 Min Read



SOURCE: LIUBOMYR VORONA VIA ALAMY STOCK PHOTO

MGM Resorts hack: How attackers hit the jackpot with service desk social engineering

Marcus White
Last updated on
November 12, 2025

When the perimeter is leaky by design

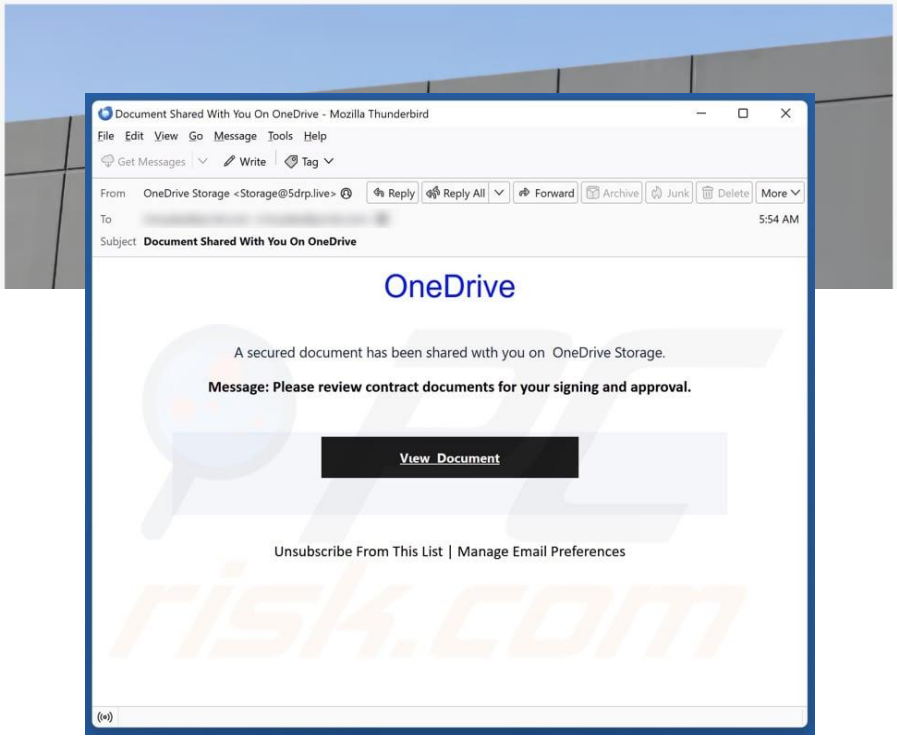
Securing inbound and outbound email

Email as target vs vector

Hillary Clinton emails - what's it all about?

6 November 2016

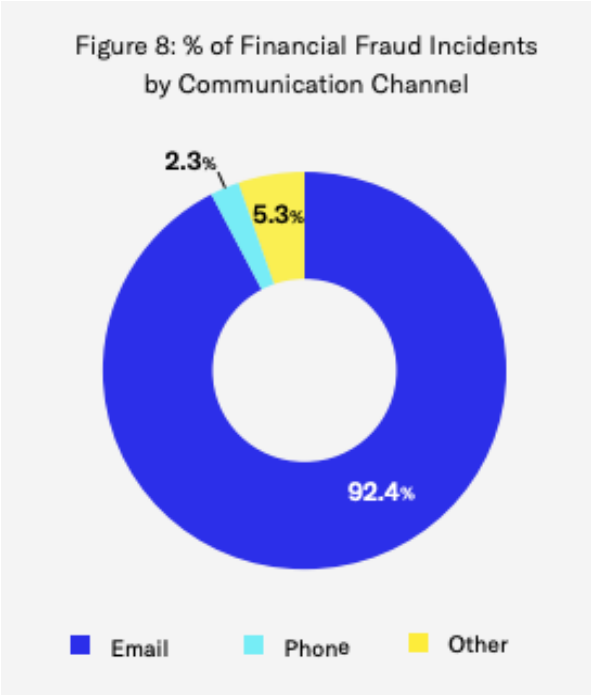
Amazon's closely guarded "Project Dawn" redundancies were accidentally exposed when a draft email from a senior AWS executive was mistakenly sent to staff



Dear Sir,
I am prince [redacted] from Nigeria. Your help would be very appreciated.
I want to transfer all of my fortune outside if Nigeria due to a frozen account,
If you could be so kind and transfer small sum of 3 500 USD to my account,
I would be able to unfreeze my account and transfer my money outside of Nigeria. To repay your kindness, I will send 1 000 000 USD to your account.

Please contact me to proceed

Prince [redacted]



https://www.at-bay.com/wp-content/uploads/2024/11/At-Bay-2024-InsurSec-Rankings-Report.pdf

Email (in)security

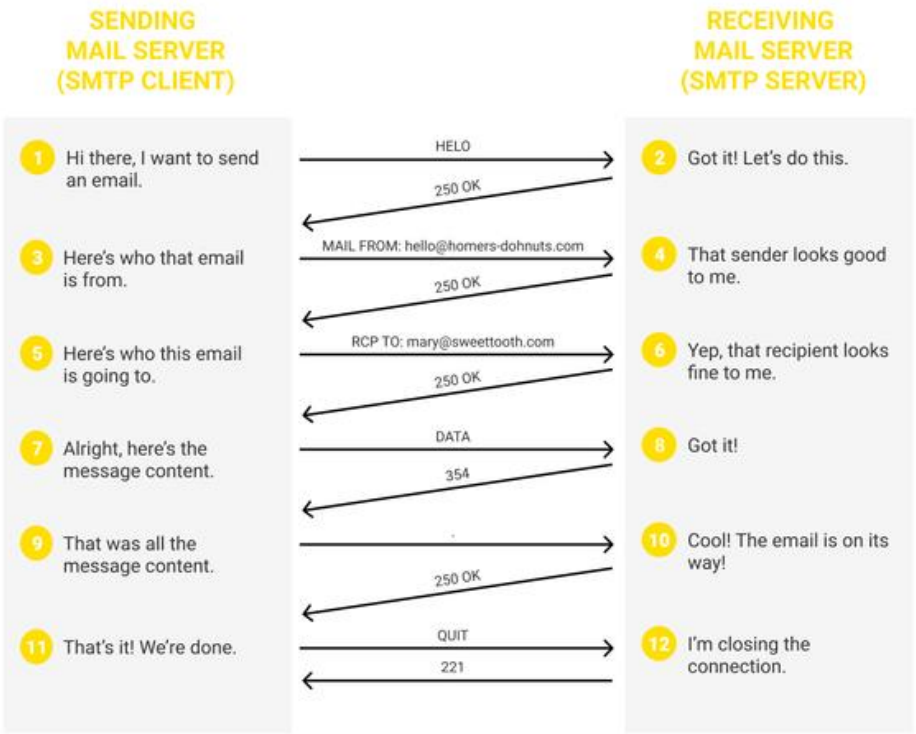


Security Engineering in 1980s

- Threat model
  - Researchers sharing research
  - Value openness
- Security mechanisms
  - "To" field secured by DNS and routing
  - Hope "From" field won't be abused

What changed and when?

- Spam abuses trust in "to" field
  - See Finn Brunton's book
  - Earliest internet harm
  - Never really fixed
- Scammers spoof "first" message from major companies
  - Spray and prey scams
  - Phishing



Securing email in transit

- Do you trust the sender or not?
  - If yes, then STARTTLS and S/MIME are enough
  - If not, then you need PGP (E2E encryption)
    - But do you trust yourself to configure
- Who even runs their own mail server these days?
  - Compare and contrast FB messenger vs gmail
  - The Intel Community likes this

[PS] Why **Johnny Can't Encrypt**: A Usability Evaluation of PGP 5.0.
A Whitten, JD Tygar - USENIX security symposium, 1999 - usenix.org
… PGP 5.0's user interface does **not** come even reasonably close to achieving our usability standard – it does **not** make public key **encryption** of electronic mail manageable for average …
☆ Save 99 Cite Cited by 2223 Related articles All 39 versions »

Authenticating Email Sender's Domain

SMTP weakness

- The envelope sender and the header From are set independently, and nothing verifies either
- Envelope: bounce@scam.com
- Header: cfo@bank.example

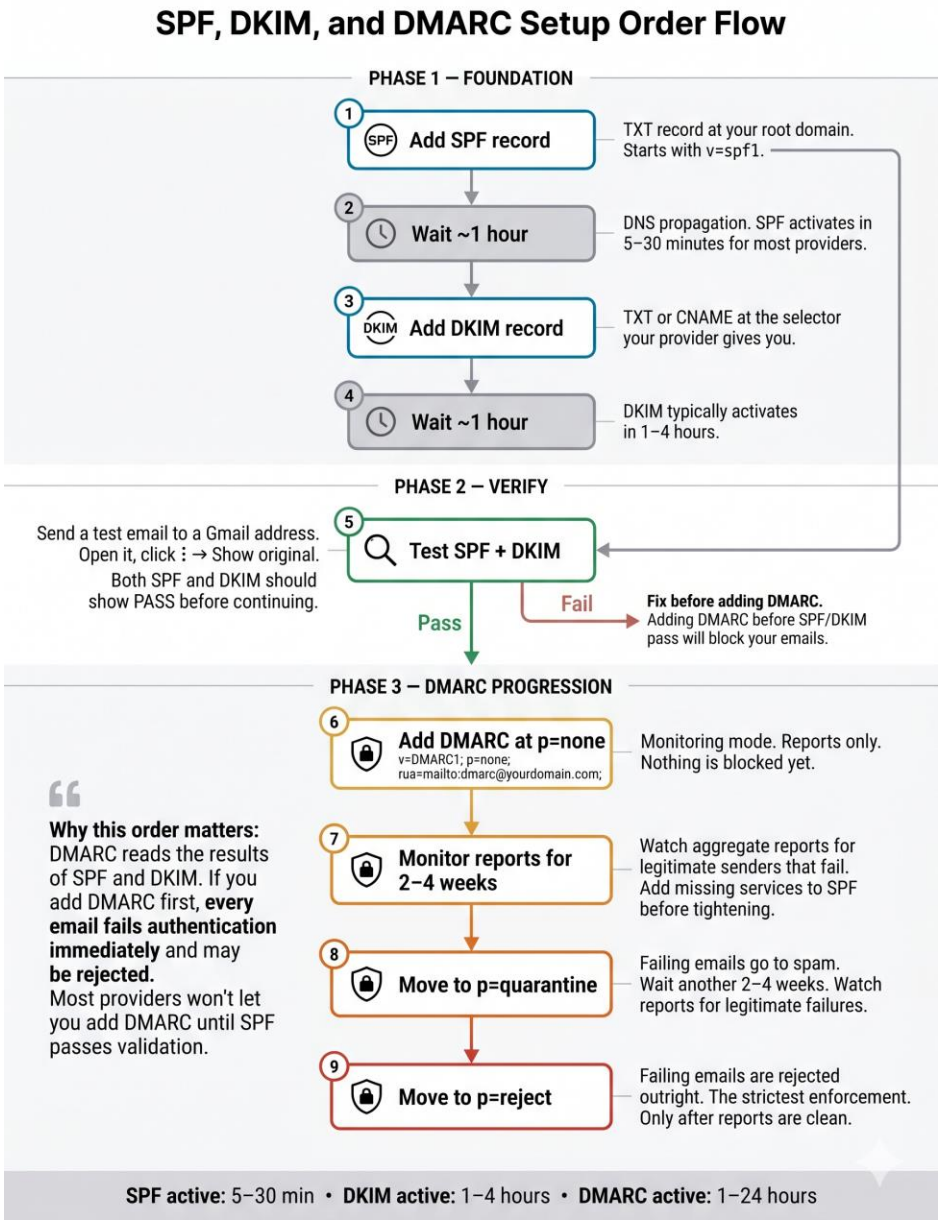
SPF and DKIM as checks

- SPF lists the IPs allowed to send and checks the envelope address
- DKIM signs headers and body

DMARC as enforcement layer

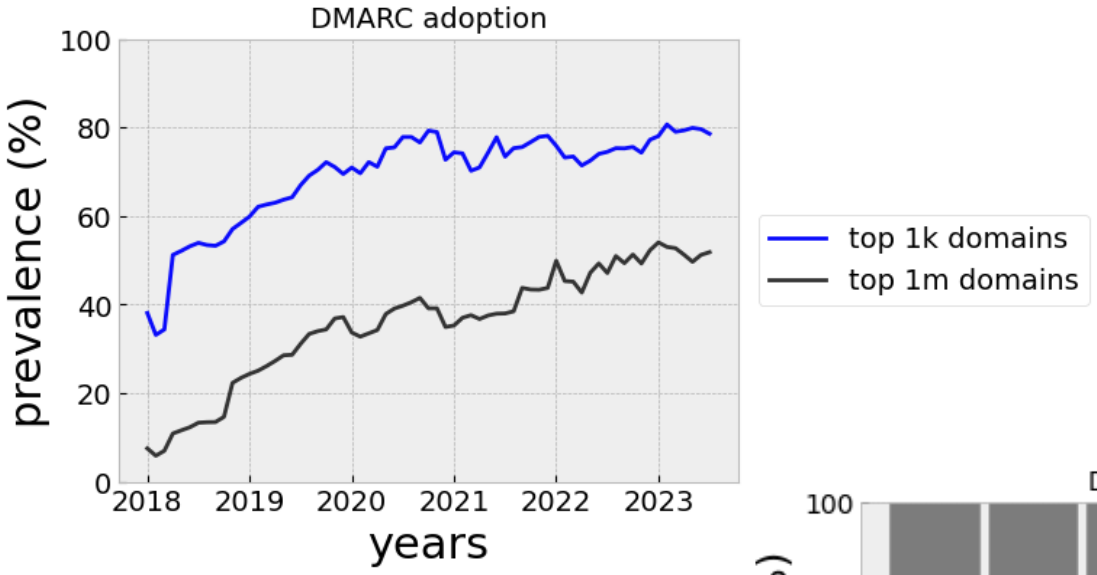
- Passes when SPF or DKIM passes and aligns with the From header
- Policy options:
  - p=none · quarantine · reject

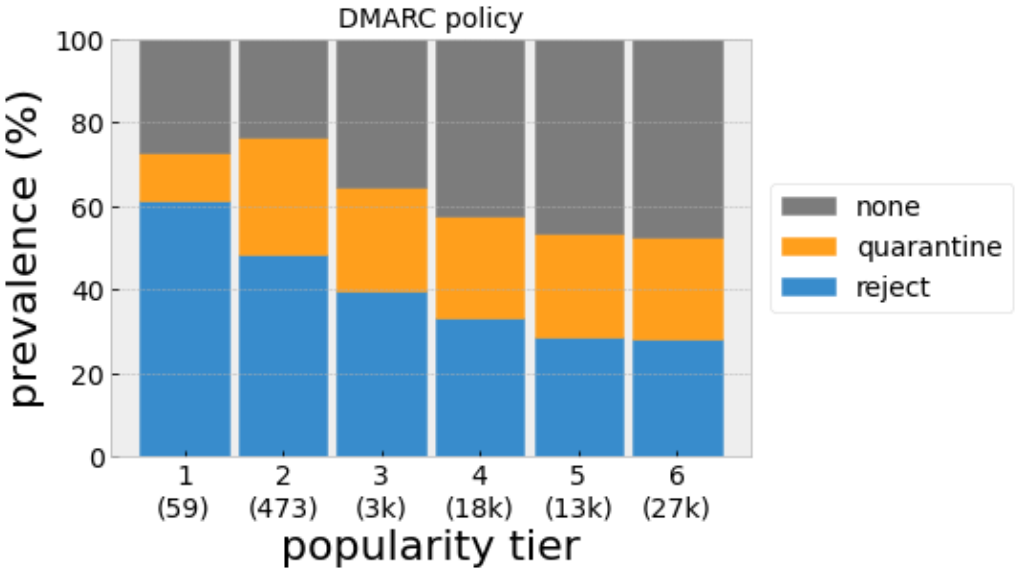
What goes wrong?



https://wpmailsmtp.com/dmarc-spf-dkim/

Adoption as a major barrier





https://www.bitsight.com/blog/domain-insecurity-state-dmarc

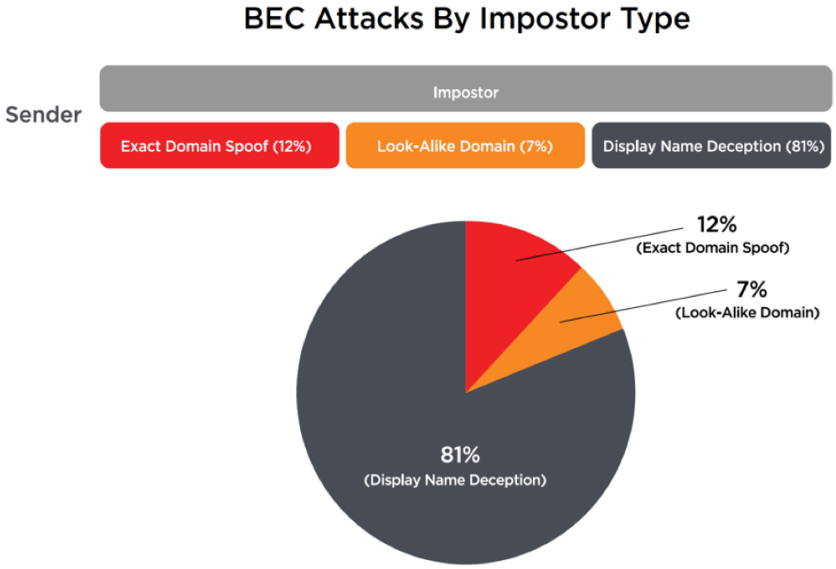
Email security as a coordination problem

- In 2024, Google and Yahoo agree bulk sender requirements
  - Marketing as a security incentive

Requirement	General Email Senders	Bulk Senders (5,000+ messages/day)
SPF/DKIM Email Authentication	Required	Both SPF and DKIM Required
Forward and Reverse DNS Records	Required	Required
TLS Connection for Transmitting Email	Required	Required
Spam Rates in Postmaster Tools	Below 0.10%, avoid 0.30% or higher	Below 0.10%, avoid 0.30% or higher
Message Format (RFC 5322)	Required	Required
Impersonating Gmail From: Headers	Prohibited (may impact email delivery)	Prohibited (may impact email delivery)
ARC Headers for Forwarded Email	Recommended for regular forwarders	Recommended for regular forwarders
List-id Header for Mailing List Senders	Recommended	Recommended
DMARC Email Authentication	Not mentioned	Required (DMARC enforcement policy can be set to none)
Alignment of From: Header with SPF/DKIM Domain	Not mentioned	Required for direct mail to pass DMARC alignment
One-Click Unsubscribe and Visible Unsubscribe Link	Not mentioned	Required for marketing and subscribed messages

What goes wrong despite DMARC

- Many allow unauthenticated emails to send (p=none)
- Even if the email domain is authenticated:
  - Lookalike domains ---> gooogle.com
  - Display name spoofing --> <Daniel Woods, daniel.woods@criminal.com>
  - 3rd party business email compromise

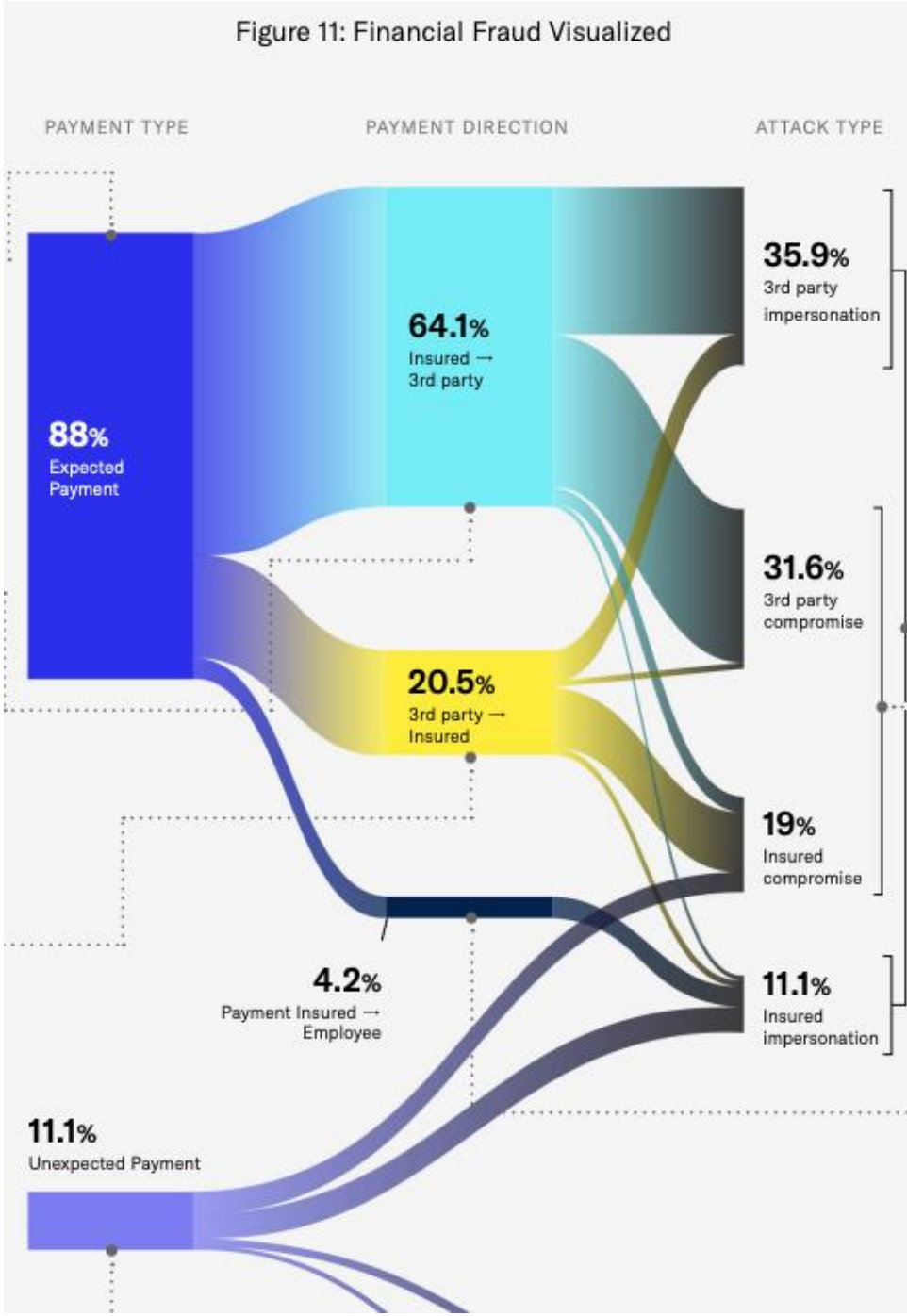


https://emailsecurity.fortra.com/blog/new-agari-report-shows-high-risk-for-bec-attacks

Email fraud

- Expected vs unexpected payments
- Who is compromised?
  - 3rd party or 1st party
- How is the 3rd party impersonated?
  - Spoof them
  - Compromise them

Read and understand Figure 11!!



What to do about email attacks

You

- Protect your inboxes
  - Strong MFA, monitor for malicious logins
- Filter out maliciousness
  - Scan links/files, block domains (e.g. newly registered?)
  - At what cost??

Your counter parties

- Protect their employees' inboxes
- Set up SPF, DKIM, DMARC (and reject)
- Register lookalike domains

When the perimeter is leaky by design

Securing web traffic

Early web security

Threat model in 1990s

- Threat model
  - Customers trying to send credit card details to ecommerce site, who intercepts along the way
- SSL as the security mechanism
  - Encrypt messages via symmetric crypto
  - Authenticate server via digital certificate w/ server's public key
  - Verify certificate was signed by trusted authority

What fails?

- Chain of trust across 100s of global CAs
  - Diginotar (2011),
- Implementation issues
  - Open SSL vulns
  - Whether apps verify certificates (source)
- Protocol issues + downgrade attacks

Fake DigiNotar web certificate risk to Iranians

5 September 2011

"Up to 300,000 Iranians may have had their Google email monitored using security certificates stolen from Dutch firm DigiNotar."



ABSTRACT

SSL (Secure Sockets Layer) is the de facto standard for secure Internet communications. Security of SSL connections against an active network attacker depends on correctly validating public-key certificates presented when the connection is established.

We demonstrate that SSL certificate validation is completely broken in many security-critical applications and libraries. Vulnerable software includes Amazon's EC2 Java library and all cloud clients based on it; Amazon's and PayPal's merchant SDKs responsible for transmitting payment details from e-commerce sites to payment gateways; integrated shopping carts such as osCommerce, ZenCart, Ubercart, and PrestaShop; AdMob code used by mobile websites; Chase mobile banking and several other Android apps and libraries; Java Web-services middleware—including Apache Axis, Axis 2, Codehaus XFire, and Pusher library for Android—and *all* applications employing this middleware. Any SSL connection from any of these programs is insecure against a man-in-the-middle attack.

The root causes of these vulnerabilities are badly designed APIs of SSL implementations (such as JSSE, OpenSSL, and GnuTLS) and data-transport libraries (such as cURL) which present developers with a confusing array of settings and options. We analyze perils and pitfalls of SSL certificate validation in software based on these APIs and present our recommendations.

Transport Layer Security (TLS)

RESEARCH-ARTICLE | FREE ACCESS

A Comprehensive Symbolic Analysis of TLS 1.3

Authors: Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott, Thyla van der Merwe | Authors Info & Claims

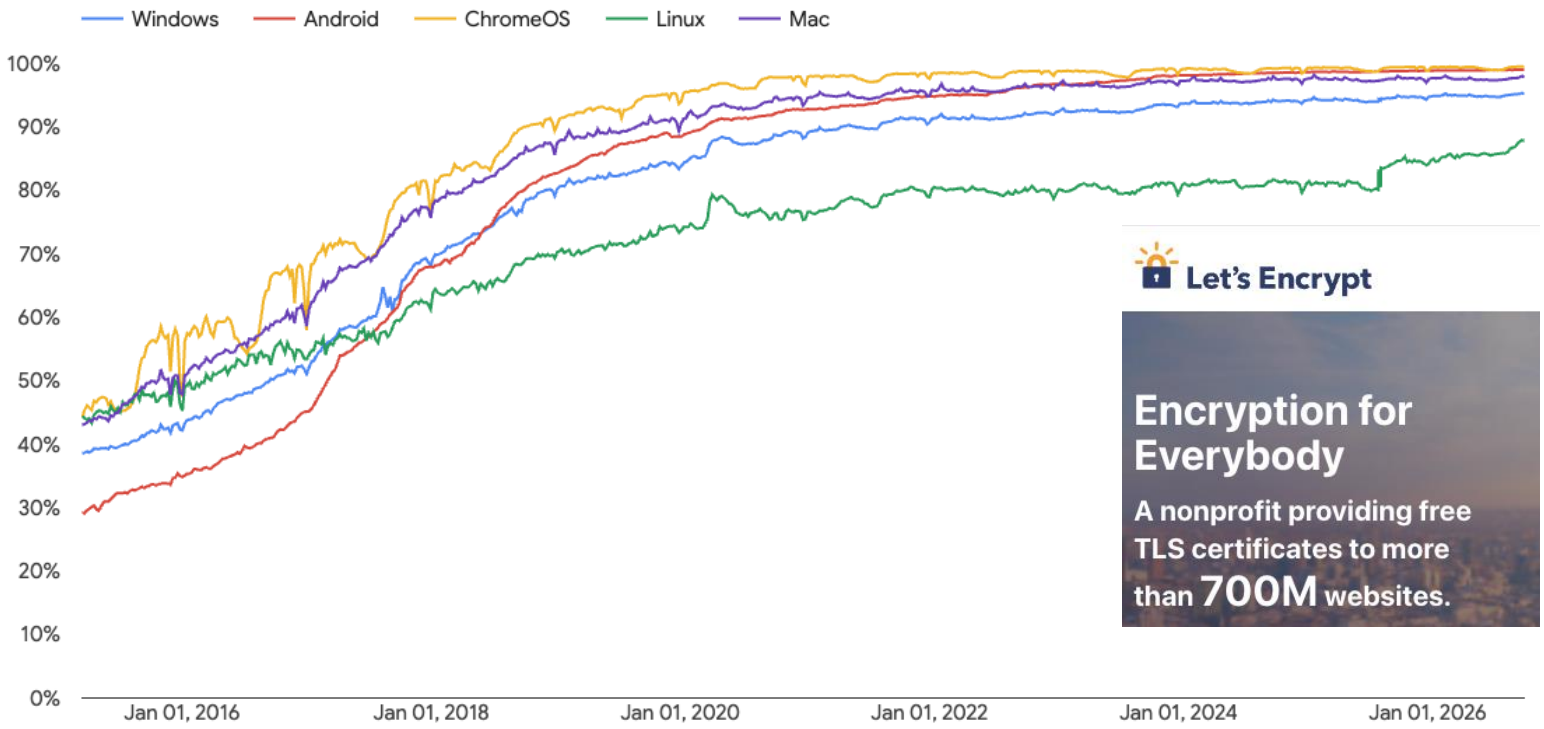
CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security
Pages 1773 - 1788 • https://doi.org/10.1145/3133956.3134063

Published: 30 October 2017 Publication History Check for updates

And similar formal verification efforts fix the protocol issues...

But what goes wrong??

Percentage of pages loaded over HTTPS in Chrome by platform



Fragment navigations, history push state navigations, and all schemes besides HTTP/HTTPS (including new tab page navigations) are not included.

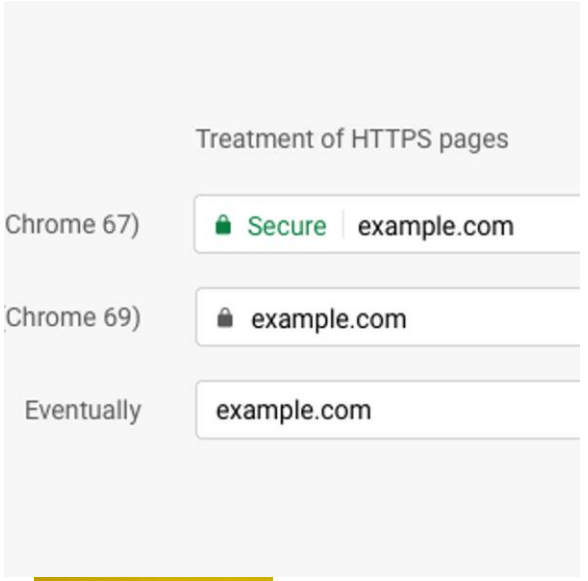
What actually goes wrong

Real-world Web Attacks

- Browser vulnerabilities
- Social engineering to click on malicious links
- Installing malware on dubious sites
- Malvertising
- ….

What does network security look like

- Blocking malicious websites and connections
  - At firewall
  - In browser
  - At email
    - See Uni and "SafeLinks" debacle
- Angry users if you get in the way!





"Non-crypto security will remain a mess" Shamir 2003

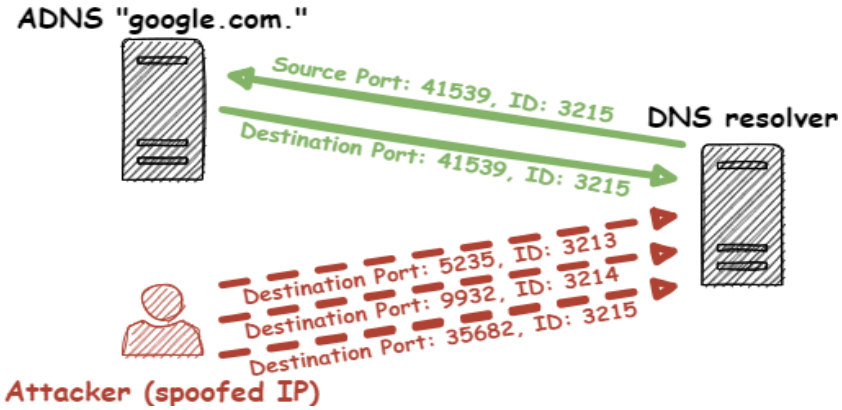
Attacks on DNS

- The "to" field depends on DNS
  - SPF/DKIM/DMARC lookups
  - Validating certificates lookups
- Designed for a cooperative network (1980s)
  - DNS responses are unauthenticated
  - Kaminsky shows a 16-bit ID was only check
  - DNSSEC, the solution, barely deployed
- Most failures come through intermediaries:
  - Registrar compromised: NYT, Twitter and others redirected via Melbourne IT (2013)
  - BGP attacks --> hijack traffic
- How does TLS interplay with DNS attacks?
  - BGP attack on MyEtherWallet.com's DNS provider, browsers flash a warning but users click through

Domain registrar Melbourne IT at center of SEA meddling with New York Times, Twitter

August 27, 2013 - 10:54 pm

"attackers gained access to the domain registration accounts that were operated by Melbourne IT, and changed the authoritative DNS servers to ns1.syrianelectronicarmy.com"



TECH CRYPTO SECURITY

Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet

by Russell Brandom

Apr 24, 2018, 6:40 PM GMT+1

Big Network Security Idea:
No matter how hard you try, perimeters are leaky bc you don't know who you're connecting with and you can't block for business reasons

Network Security Summary

- Security was largely absent from early internet
  - Had to be layered on via firewalls/DMARC/TLS etc
  - DDoS mostly solved by professional hosting
- Perimeterisation based on network address fails
  - Zero trust, "identity is the new perimeter" etc etc
- Security in transit largely solved by TLS
  - Initially faced adoption challenge, pushed by browser vendors
  - Pushes attacks to authentication (not unlike banking)
    - BEC for financial fraud
    - Compromise web server, or certificate authority for web attacks
- Simplest attacks need no compromise, but a new domain
  - Finance employees fail to spot lookalike domains/display name spoofing
  - General users click phishing links/navigate to malware
- Blocking isn't an option from business PoV
  - Hence DMARC (p=none), hence allowing arbitrary links